PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-228519

(43)Date of publication of application : 15.08.2003

(51)Int.Cl. G06F 12/14
G06F 12/00
G06F 15/00
G09C 1/00
H04L 9/08
H04L 9/32

(21)Application number : 2002-359960

(22)Date of filing : 11.12.2002

(71)Applicant : PERVASIVE SECURITY SYSTEMS INC

(72)Inventor : ROSSMANN ALAIN
ZUILI PATRICK
OUYE MICHAEL MICHIO
HUMPICH SERGE
LEE CHANG-PING
VAINSTEIN KLIMENTY
HILDERBRAND HAL
GARCIA DENIS JACQUES PAUL
SUPRAMANIAM SENTHILVASAN
HUANG WEIQING
RYAN NICHOLAS MICHAEL

(30)Priority

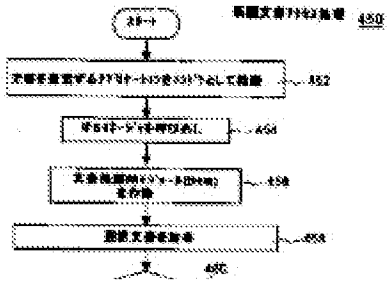
Priority number	Priority date	Priority country
2001 339634	12.12.2001	US
2002 076254	12.02.2002	US

(54) METHOD AND ARCHITECTURE FOR PROVIDING PERVASIVE SECURITY FOR DIGITAL ASSET

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a technique that gives pervasive security to digital assets.

SOLUTION: A server is configured to provide access control (AC) management for a user (for example, a



single user, and a group of users, software agents or devices) with a need to access secured data. In a server module, many access rules for the secured data and/or access privileges for the user are created, updated and managed so that a user given an appropriate access privilege can access a secured document if granted by a corresponding access rule in the secured data.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－228519
（P2003－228519A）
(43)公開日　平成15年８月15日(2003.8.15)

(51)Int.Cl.[7]		識別記号	FI		テーマコード（参考）
Ｇ０６Ｆ	12/14	３１０	Ｇ０６Ｆ 12/14	３１０Ｋ	５Ｂ０１７
		３２０		３２０Ｂ	５Ｂ０８２
	12/00	５３７	12/00	５３７Ａ	５Ｂ０８５
	15/00	３３０	15/00	３３０Ａ	５Ｊ１０４
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ 1/00	６４０Ｅ	

審査請求　未請求　請求項の数46　ＯＬ　（全 39 頁）　最終頁に続く

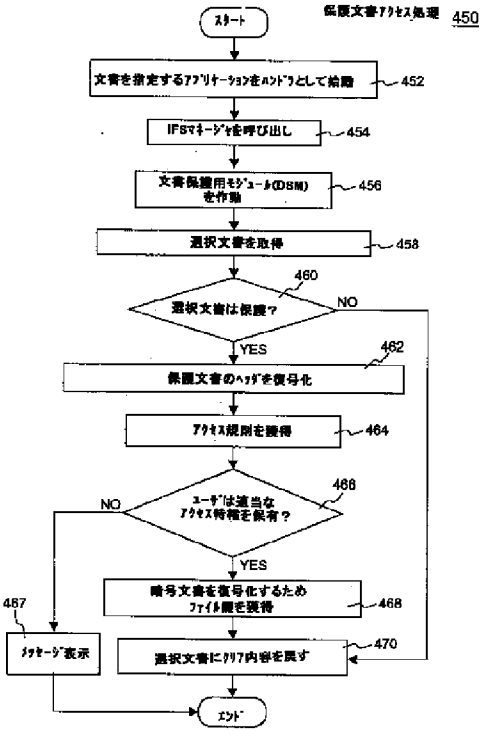
(21)出願番号　特願2002－359960(P2002－359960)
(22)出願日　平成14年12月11日(2002.12.11)
(31)優先権主張番号　３３９６３４
(32)優先日　平成13年12月12日(2001.12.12)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　０７６２５４
(32)優先日　平成14年２月12日(2002.2.12)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　502448498
パーヴェイシヴ　セキュリティー　システムズ　インコーポレイテッド
Ｐｅｒｖａｓｉｖｅ　Ｓｅｃｕｒｉｔｙ　Ｓｙｓｔｅｍｓ，　Ｉｎｃ．
アメリカ合衆国　カリフォルニア州　94025　メンロー・パーク　ミドルフィールド・ロード　535　スイート・120
(74)代理人　100070150
弁理士　伊東　忠彦　（外２名）

最終頁に続く

(54)【発明の名称】　デジタル資産にパーベイシブ・セキュリティを提供する方法及びアーキテクチャ

(57)【要約】
【課題】　本発明は、デジタル資産にパーベイシブ・セキュリティを付与する技術の提供を目的とする。
【解決手段】　本発明の一局面によれば、サーバは、保護データにアクセスする必要があるユーザ（例えば、単独ユーザ、ユーザのグループ、ソフトウェア・エージェント、又は、装置）にアクセス制御（ＡＣ）マネージメントを行うように構成される。サーバ・モジュール内では、保護データのための多数のアクセス規則及び／又はユーザのためのアクセス特権が作成、更新、及び、管理され、適当なアクセス特権が与えられたユーザは、保護データ内の対応したアクセス規則で許可された場合、保護文書にアクセスできる。



【特許請求の範囲】
【請求項１】　電子データにアクセス制御マネージメントを行う方法であって、
電子データはセキュリティ情報と暗号データ部とを含むフォーマットで保護され、セキュリティ情報は暗号化され、対応した暗号データ部へのアクセスを制御するようにされ、
電子データにアクセスするクライアント装置のユーザを識別する識別子を含む認証要求をクライアント装置から受信したとき、クライアント装置との間で安全なリンクを確立する手順と、
識別子に応じてユーザを認証する手順と、
ユーザが認証された後に、暗号化されたセキュリティ情報を復号化するため使用されるユーザ鍵を有効状態にする手順と、を有する方法。
【請求項２】　アクセス制御マネージメントを維持する手順を更に有し、
アクセス制御マネージメントは、
電子データに対する少なくとも１組の規則を含む規則マネージャと、
運営者が電子データに対する指定場所のための規則を管理するため用いる管理インタフェースと、を具備している、請求項１記載の方法。
【請求項３】　規則マネージャは、規則を作成、管理、又は、更新するため使用するグラフィック・ユーザ・インタフェースを提供する、請求項２記載の方法。
【請求項４】　グラフィック・ユーザ・インタフェースから規則を判定するパラメータは、次に、マークアップ言語で表現される、請求項３記載の方法。
【請求項５】　アクセス制御マネージメントは、認証されたユーザのリスト、及び、認証された各ユーザに関連したアクセス特権を収容するデータベースに接続されたユーザ・マネージャを更に具備する、請求項２記載の方法。
【請求項６】　ユーザを認証する手順は、
ユーザに関してデータベースを調べる手順と、
ユーザに関する情報がデータベースに存在した場合に、データベースから、ユーザが電子データにアクセスすることが許可されている場所に関するアクセスロケーション情報を取得する手順と、を含む、請求項１乃至５のうちいずれか一項記載の方法。
【請求項７】　識別子はクライアント装置を更に識別し、
ユーザを認証する手順は、
アクセスロケーション情報に基づいて、ユーザがクライアント装置から電子データにアクセスすることを許可されているかどうかを判定する手順を含む、請求項６記載の方法。
【請求項８】　ユーザ鍵はクライアント装置に置かれ、
ユーザ鍵を有効状態にする手順は、
認証メッセージをクライアント装置へ送信する手順と、
認証メッセージでユーザ鍵を有効状態にする手順と、を含む、請求項１乃至５のうちいずれか一項記載の方法。
【請求項９】　セキュリティ情報は、アクセス規則の組及びファイル鍵を含み、
ユーザのアクセス特権がアクセス規則によって合格していると評価された場合に限り、ファイル鍵は暗号データ部を復号化するために取り出すことが可能である、請求項１乃至５のうちいずれか一項記載の方法。
【請求項１０】　保護された電子データは、暗号化されたセキュリティ情報を収容するヘッダ、及び、電子データが保護されていることを示す署名を含み、
暗号化されたセキュリティ情報は、アクセス規則の組、及び、ファイル鍵を含み、
クライアント装置からヘッダを受け取る手順と、
アクセス規則を取り出すため、ヘッダ内のセキュリティ情報を復号化する手順と、
アクセス規則がユーザのアクセス特権に対して合格であると評価されたとき、ファイル鍵を取り出す手順と、を更に有する請求項１記載の方法。
【請求項１１】　ファイル鍵をクライアント装置へ送信する手順を更に有し、
暗号データ部は、クライアント装置で実行される暗号モジュールによってファイル鍵で復号化することができる、請求項１０記載の方法。
【請求項１２】　電子データにアクセス制御マネージメントを行う方法であって、
電子データにアクセスしようとするユーザを認証する手順と、
ユーザに関連付けられた秘密鍵及び公開鍵を保持する手順と、を有し、
電子データは、保護されると、セキュリティ情報を収容したヘッダ、及び、暗号データ部を含み、
電子データが記憶装置に書き込まれるとき、公開鍵でセキュリティ情報を暗号化する手順と、
電子データがアプリケーションによってアクセスされるとき、秘密鍵でセキュリティ情報を復号化する手順と、を有する方法。
【請求項１３】ユーザを認証する手順は、
ユーザが電子データにアクセスしようとしているクライアント装置との間にリンクを確立する手順と、
ユーザからの資格情報を要求する手順と、
安全なリンクを介してクライアント装置から資格情報を受信する手順と、を含む、請求項１２記載の方法。
【請求項１４】　公開鍵でセキュリティ情報を暗号化する手順は、
アクセス規則、及び、クライアント装置で暗号データ部を生成するため使用されたファイル鍵を受け取る手順と、
アクセス規則及びクライアント鍵をセキュリティ情報に

組み込む手順と、
公開鍵でセキュリティ情報を暗号化する手順と、を含む、請求項１２又は１３記載の方法。
【請求項１５】　暗号化されたセキュリティ情報を収容するヘッダを生成する手順と、
暗号データ部と一体化されたヘッダをクライアント装置へアップロードする手順と、を更に有する請求項１４記載の方法。
【請求項１６】　アクセス規則はマークアップ言語で表現されている、請求項１４記載の方法。
【請求項１７】　秘密鍵でセキュリティ情報を復号化する手順は、
リンクを介してクライアント装置からヘッダを受信する手順と、
ヘッダからセキュリティ情報を解析する手順と、
秘密鍵でセキュリティ情報を復号化する手順と、を含む、請求項１２記載の方法。
【請求項１８】　セキュリティ情報からアクセス規則を取得する手順と、
アクセス規則がユーザのアクセス特権を受け入れるかどうかを判定する手順と、
判定に合格したとき、
セキュリティ情報からファイル鍵を取り出す手順と、
リンクを介してファイル鍵をクライアント装置へ送信する手順と、
判定に合格しなかったとき、
リンクを介してエラーメッセージをクライアント装置へ送信する手順と、を更に有する請求項１７記載の方法。
【請求項１９】　電子データにアクセス制御マネージメントを行う方法であって、
アプリケーションによる電子データにアクセスするための要求を受け取る手順と、
電子データのセキュリティ特性を判定する手順と、を有し、
電子データは保護されていることがセキュリティ特性からわかったとき、電子データは、セキュリティ情報を収容するヘッダ、及び、暗号データ部を含み、
セキュリティ情報に基づいて、ユーザが暗号データ部にアクセスするために必要なアクセス特権を与えられているかどうかを判定する手順と、
ユーザは暗号データ部にアクセスするために必要なアクセス特権を与えられていると判定された後に限り、暗号データ部を復号化する手順と、を更に有する方法。
【請求項２０】　セキュリティ情報に基づいてユーザが必要なアクセス特権を与えられているかどうかを判定する手順は、
ユーザ鍵でセキュリティ情報を復号化する手順と、
セキュリティ情報からアクセス規則を取り出す手順と、
アクセス規則をユーザのアクセス特権と比較する手順と、を含む、請求項１９記載の方法。
【請求項２１】　アクセス規則とアクセス特権の比較に合格した場合、セキュリティ情報からファイル鍵を取り出す手順を更に有する請求項２０記載の方法。
【請求項２２】　アクセス制御マネージメントを実行するサーバとの間にリンクを確立する手順と、
アクセス制御マネージメントがユーザを認証するため、ユーザを識別する識別子を含む認証要求をサーバへ送信する手順と、
ヘッダをサーバへ転送する手順と、
ヘッダから取り出されたファイル鍵を受け取る手順と、を更に有する請求項１９記載の方法。
【請求項２３】　暗号モジュールを作動する手順と、
受け取られたファイル鍵を用いて暗号モジュールによって暗号データ部を復号化する手順と、を更に有する請求項２２記載の方法。
【請求項２４】　アクセス制御マネージメントを実行するサーバとの間にリンクを確立する手順と、
アクセス制御マネージメントがユーザを認証するため、ユーザを識別する識別子を含む認証要求をサーバへ送信する手順と、
ユーザが認証された後、認証メッセージを受信する手順と、
クライアント装置内で局部的にユーザ鍵を有効状態にする手順と、を更に有する請求項１９記載の方法。
【請求項２５】　電子データにアクセス制御マネージメントを行うシステムであって、
電子データが選択されたときに通過させられるパスで動作し、電子データのセキュリティ特性を判定する文書保護用モジュールを実行するクライアント装置と、
ネットワークを介してクライアント装置に接続され、電子データにアクセスする全ユーザを管理するアカウント・マネージャを含むアクセス制御サーバと、を有し、
クライアント装置及び／又はクライアント装置のユーザは、電子データが保護されていることがセキュリティ特性によって示されるとき、文書保護用モジュールによってアクセス制御サーバで認証され、
保護された電子データのアクセス規則はユーザに関連したユーザ鍵で取り出される、システム。
【請求項２６】　アクセス規則はユーザのアクセス特権と比較される、請求項２５記載のシステム。
【請求項２７】　ユーザのアクセス特権はアクセス規則によって許可されていることが文書保護用モジュールによって判定された後、文書保護用モジュールは、保護された電子データの暗号データ部を保護された電子データから獲得されたファイル鍵で復号化するため、暗号モジュールを作動する、請求項２６記載のシステム。
【請求項２８】　ユーザ鍵は、保護された電子データの一部を受け取るアクセス制御サーバに保持され、
アクセス規則及びファイル鍵は、保護された電子データの一部から取得される、請求項２８記載のシステム。

【請求項２９】　アクセス制御サーバはネットワークを介してファイル鍵をクライアント装置へ転送する、請求項２５記載のシステム。
【請求項３０】　ユーザ鍵はクライアント装置に維持され、クライアント装置及びユーザの両方がアクセス制御サーバによって認証されたとき、ユーザ鍵が有効状態にされる、請求項２５記載のシステム。
【請求項３１】　電子データにアクセス制御マネージメントを行うシステムであって、
保護された電子データは暗号セキュリティ情報を含み、暗号セキュリティ情報は少なくともアクセス規則の組とファイル鍵を含み、
保護された電子データを保持するため指定された少なくとも有効な場所を収容する記憶装置と、
記憶装置に接続され、アプリケーションによって選択されたときに有効な場所から電子データが通過させられるパス内で動作する文書保護用モジュールを実行するクライアント装置と、
ネットワークを介してクライアント装置に接続され、クライアント装置から暗号セキュリティ情報を含む電子データの一部を受信するアクセス制御サーバと、を有し、
ユーザとクライアント装置の両方が認証された後、暗号セキュリティ情報は、電子データにアクセスするためクライアント装置内でアプリケーションを実行するユーザと関連付けられたユーザ鍵で復号化され、
アクセス規則の組はアクセス制御サーバ内のユーザのアクセス特権と比較され、合格した場合に、電子データをクリアモードで復元することを容易に実現させるためのファイル鍵がクライアント装置へ返される、システム。
【請求項３２】　電子データにアクセス制御マネージメントを行うプログラムであって、
電子データにアクセスするクライアント装置のユーザを識別する識別子を含む認証要求をクライアント装置から受信したとき、クライアント装置との間で安全なリンクを確立する機能と、
識別子に応じてユーザを認証する機能と、
ユーザが認証された後に、暗号化されたセキュリティ情報を復号化するため使用されるユーザ鍵を有効状態にする機能と、をコンピュータに実現させるためのプログラム。
【請求項３３】　アクセス制御マネージメントを維持する機能を更に有し、
アクセス制御マネージメントは、
電子データに対する少なくとも１組の規則を含む規則マネージャと、
運営者が電子データに対する指定場所のための規則を管理するため用いる管理インタフェースと、を具備している、請求項３２記載のプログラム。
【請求項３４】　アクセス制御マネージメントは、認証されたユーザのリスト、及び、認証された各ユーザに関連したアクセス特権を収容するデータベースに接続されたユーザ・マネージャを更に具備する、請求項３２又は３３記載のプログラム。
【請求項３５】　ユーザを認証する機能は、
ユーザに関してデータベースを調べる機能と、
ユーザに関する情報がデータベースに存在した場合に、データベースから、ユーザが電子データにアクセスすることが許可されている場所に関するアクセスロケーション情報を取得する機能と、を含む、請求項３４記載のプログラム。
【請求項３６】　電子データにアクセス制御マネージメントを行うプログラムであって、
電子データにアクセスしようとするユーザを認証する機能と、
ユーザに関連付けられた秘密鍵及び公開鍵を保持する機能と、をコンピュータに実現させ、
電子データは、保護されると、セキュリティ情報を収容したヘッダ、及び、暗号データ部を含み、
電子データが記憶装置に書き込まれるとき、公開鍵でセキュリティ情報を暗号化する機能と、
電子データがアプリケーションによってアクセスされるとき、秘密鍵でセキュリティ情報を復号化する機能と、を更にコンピュータに実現させるためのプログラム。
【請求項３７】ユーザを認証する機能は、
ユーザが電子データにアクセスしようとしているクライアント装置との間にリンクを確立する機能と、
ユーザからの資格情報を要求する機能と、
安全なリンクを介してクライアント装置から資格情報を受信する機能と、を含む、請求項３６記載のプログラム。
【請求項３８】　公開鍵でセキュリティ情報を暗号化する機能は、
アクセス規則、及び、クライアント装置で暗号データ部を生成するため使用されたファイル鍵を受け取る機能と、
アクセス規則及びクライアント鍵をセキュリティ情報に組み込む機能と、
公開鍵でセキュリティ情報を暗号化する機能と、
を含む、請求項３６又は３７記載のプログラム。
【請求項３９】　暗号化されたセキュリティ情報を収容するヘッダを生成する機能と、
暗号データ部と一体化されたヘッダをクライアント装置へアップロードする機能と、を更にコンピュータに実現させるための請求項３８記載のプログラム。
【請求項４０】　秘密鍵でセキュリティ情報を復号化する機能は、
リンクを介してクライアント装置からヘッダを受信する機能と、
ヘッダからセキュリティ情報を解析する機能と、
秘密鍵でセキュリティ情報を復号化する機能と、を含

む、請求項３９記載のプログラム。
【請求項４１】　セキュリティ情報からアクセス規則を取得する機能と、
アクセス規則がユーザのアクセス特権を受け入れるかどうかを判定する機能と、
判定に合格したとき、
セキュリティ情報からファイル鍵を取り出す機能と、
リンクを介してファイル鍵をクライアント装置へ送信する機能と、
判定に合格しなかったとき、
リンクを介してエラーメッセージをクライアント装置へ送信する機能と、を更にコンピュータに実現させるための請求項４０記載のプログラム。
【請求項４２】　電子データにアクセス制御マネージメントを行うプログラムであって、
アプリケーションによる電子データにアクセスするための要求を受け取る機能と、
電子データのセキュリティ特性を判定する機能と、をコンピュータに実現させ、
電子データは保護されていることがセキュリティ特性からわかったとき、電子データは、セキュリティ情報を収容するヘッダ、及び、暗号データ部を含み、
セキュリティ情報に基づいて、ユーザが暗号データ部にアクセスするために必要なアクセス特権を与えられているかどうかを判定する機能と、
ユーザは暗号データ部にアクセスするために必要なアクセス特権を与えられていると判定された後に限り、暗号データ部を復号化する機能と、を更にコンピュータに実現させるためのプログラム。
【請求項４３】　要求を行ったユーザに関連したユーザ鍵を取り出す機能を更にコンピュータに実現させるための請求項４２記載のプログラム。
【請求項４４】　セキュリティ情報に基づいてユーザが必要なアクセス特権を与えられているかどうかを判定する機能は、
ユーザ鍵でセキュリティ情報を復号化する機能と、
セキュリティ情報からアクセス規則を取り出す機能と、
アクセス規則をユーザのアクセス特権と比較する機能と、を含む、請求項４２又は４３記載のプログラム。
【請求項４５】　アクセス規則とアクセス特権の比較に合格した場合、セキュリティ情報からファイル鍵を取り出す機能を更にコンピュータに実現させるための請求項４４記載のプログラム。
【請求項４６】　アクセス規則とアクセス特権の比較に合格しなかった場合、クライアント装置がユーザに対してエラーメッセージを表示する機能を更にコンピュータに実現させるための請求項４５記載のプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、企業環境におけるデータ保護の分野に係わり、特に、あらゆるときにデジタル資産にセキュリティを提供する処理、システム、アーキテクチャ、ソフトウェア製品、及び、プログラムに関する。
【０００２】
【従来の技術】インターネットは、歴史上、最速に発展している通信媒体である。このようなインターネットの発展と、インターネットへのアクセスの容易性は、公的部門及び私的部門の両方で最新情報テクノロジーを使用する機会を著しく増大させた。このため、ビジネスと個人の間で相互作用及びデータ共用の前例の無い機会が得られる。しかし、インターネットによって得られる利点は、情報の信頼性と完全性に対する危険の非常に大きい要素を伴う。インターネットは、広く開かれた、公衆の国際的な相互接続されたコンピュータ及び電子装置のネットワークである。適切なセキュリティ手段が無い場合、許可されていない人、又は、許可されていない機械は、インターネット上を伝わる情報を傍受し、場合によっては、一般には公衆から利用することができないインターネットに相互接続されたコンピュータに蓄積された機密情報を手に入れることができる。
【０００３】インターネット上を移動する機密情報を保護し、機密情報を保持するコンピュータへのアクセスを制限することを目的とした数多くの試みが進行中である。暗号化は、物理的世界で発見した信頼を電子的世界に持ち込むことを可能にさせるので、人々は、詐欺や偽装に惑わされること無く、ビジネスを電子的に遂行することができる。毎日、何十万人もの人々が、電子メール、電子商取引（インターネット上で行われるビジネス）、ＡＴＭ機械、或いは、携帯電話機等を通じて電子的に相互交流する。電子的に伝達される情報の増加が認められる、暗号技術への依存が増大することにつながる。
【０００４】インターネット上を伝わる機密情報を保護する際に進行中の一つの試みは、インターネット上の２台の通信中のコンピュータ間で非公開（プライベート）通信セッションを保証するため、一つ以上の暗号技術を使用することである。暗号技術は、通信チャネル上を盗聴する者に情報の内容を開示することなく、不確かな通信チャネルを介して情報を伝達する一つの方法を提供する。暗号技術に暗号化プロセスを使用すると、一方の当事者は、送信中のデータの内容を許可されていない第三者によるアクセスから保護することが可能であり、しかも、対象とする当事者（相手方）は、対応した復号化プロセスを使用してデータを読むことが可能である。
【０００５】ファイアウォールは、私設ネットワークのリソースを他のネットワークのユーザから保護する別のセキュリティ手段である。しかし、機密情報に対する多数の許可されていないアクセスは、外部からではなく、内部で行われている、ということが報告されている。あ

る人が内部から許可されていないアクセスを行う一例は、制限付き情報又は機密情報が組織内のアクセスする筈の無い人によってアクセスされるときである。インターネットの公開性のため、契約上の情報、顧客データ、幹部連絡事項、製品仕様、及び、他の極秘情報及び機密知的財産のホストは、利用可能な状態のままにされ、保護されている筈の境界内若しくは境界の外側の許可されていない人による不適当なアクセス及び使用に無防備である。

【０００６】会計検査院（ＧＡＯ）からの政府報告には、「米国商務省内の７機関で重大かつ広範囲のコンピュータ・セキュリティ上の脆弱性が見つかり、機関全体に広く行き渡ったコンピュータ・セキュリティ上の脆弱性は、機関の最も繊細なシステムの一部の完全性を著しく危険に晒す。」のように記載されている。さらに、この政府報告には、「容易に入手可能なソフトウェア及び一般的な技術を使用することによって、商取引内部から、並びに、インターネットのように遠隔的に、繊細な商取引システムに侵入できることが実証された。」、並びに、「商取引の内部及び外部の両方の個人は、これらのシステムに許可されていないアクセスを行い、細心の注意を払うべき経済的データ、財政的データ、人事データ、及び、極秘ビジネスデータなどを読み、コピーし、修正し、削除し得た。」と報告されている。この政府報告は、「侵入者は、省の使命にとって重大なシステムの運営を妨害することが可能である。」と結論付けている。

【０００７】

【発明が解決しようとする課題】実際上、殆どのビジネス及び機関は、それらの機密情報を保護するための効果的な方法を探し求めている。典型的に、ビジネス及び機関は、保護を実現するため、ファイアウォール、仮想プライベート・ネットワーク（ＶＰＮ）、及び、侵入発見システム（ＩＤＳ）などを配備している。残念ながら、これらの様々なセキュリティ手段は、プライベート・ネットワークに存在する機密情報を高信頼性で保護するためには不十分であることが判明している。例えば、細心の注意を払うべき文書にアクセスするためのパスワードに依存して、数個の文字数長のパスワードが漏洩し、或いは、見つけられたとき、屡々、安全が侵犯される。したがって、常にデジタル資産を保証し、保護するためのより効果的な方法を提供することが望まれる。

【０００８】本発明の一つの目的は、常に保護デジタル資産を守ることができる汎用保護機構を提供することである。

【０００９】

【課題を解決するための手段】本発明の幾つかの局面の概要を説明するため、好ましい実施例の一部を簡単に紹介する。概要を説明する目的を明確にするため、この欄の記載では、簡単化若しくは省略がなされている。しかし、このような簡単化若しくは省略は、本発明の有効範囲を制限するためのものではない。

【００１０】本発明は、デジタル資産に対して常にパーベイシブ・セキュリティを与える方法、システム、アーキテクチャ及びソフトウェア製品に係わり、特に、企業環境に適している。一般的に、パーベイシブ・セキュリティとは、デジタル資産が常に保護され、適切なアクセス権限若しくは特権を付与された認証されたユーザだけによってアクセスされ得ることを意味する。ここで、デジタル資産の例として、多種多様な文書、マルチメディアファイル、データ、実行可能コード、画像及びテキストが含まれるが、これらの例に限定されるものではない。

【００１１】本発明の一局面によれば、サーバ・コンピュータで実行可能なサーバ・モジュールは、アクセス制御マネージメントの下で保護された保護文書にアクセスする必要のあるユーザのグループ、ソフトウェアエージェント、若しくは、デバイスに対してアクセス制御（ＡＣ）マネージメントを行うように構成される。サーバ・モジュール内では、保護文書に対する各種のアクセス規則、及び／又は、ユーザ若しくはソフトウェアエージェントに対するアクセス特権が作成され、更新され、管理されるので、適当なアクセス特権をもつユーザ、ソフトウェアエージェント、若しくは、デバイスは、保護文書内の対応したアクセス規則によって許可されるならば、保護文書にアクセスすることができる。一実施例によれば、保護文書には、ヘッダ及び暗号化されたデータ部（暗号データ部）が含まれる。ヘッダは、暗号データ部へのアクセスを制御するための暗号化されたセキュリティ情報（暗号セキュリティ情報）を含む。暗号セキュリティ情報を復号するためには、認証されたユーザに関連したユーザ鍵を取得しなければならない。セキュリティ情報を利用できるようになると、アクセス規則がセキュリティ情報から取得され、保護文書にアクセスしているユーザのアクセス特権と比較される。この比較に合格すると、ファイル鍵がセキュリティ情報から取得され、暗号データ部を復号化するため使用され、続いて、ユーザは保護文書の保護されていないクリア文書を入手できるようになる。

【００１２】本発明の他の局面によれば、アクセス制御マネージメントは分散形式で実行される。多数のローカル・サーバ・コンピュータが、集中アクセス制御マネージメントの役割を担う中央サーバの代わりに大部分機能する。このような分散形式は、中央サーバによって行われるアクセス制御管理の信頼性、確実性及び拡張性（スケーラビリティ）を保証する。一実施例によれば、キャッシュ版のサーバ・モジュールがローカル・サーバにロードされ、実行される。その結果として、クライアント装置は、保護文書にアクセスするとき、中央サーバとライブで交信（コンサルテーション）する必要がない。中

央サーバが停止しているとき、或いは、中央サーバへのコネクションが利用できない場合でも、保護文書にアクセスすることが可能になる。

【００１３】本発明の他の局面によれば、局所的なローカル版のローカル・サーバがユーザの現在位置に応じて動的に再構成され得る。一実施例によれば、ローカル版のローカル・サーバは、ローカル・サーバの近くにあるか、或いは、ローカル・サーバによって認証済みのユーザ、ソフトウェアエージェント若しくはデバイスだけのために機能する。ユーザがある場所から別の場所へ移動するとき、前の場所から移動したユーザの新しい場所を検出した後、新しい場所に対するローカル版のローカル・サーバは、そのユーザへのサポートを追加するように再構成され、同時に、前の場所に対するローカル版のローカル・サーバは、そのユーザに対するサポートを取り除くように再構成される。その結果として、セキュリティが向上し、あるユーザに許可されるアクセス権は、組織に属する場所の個数や、そのユーザに許可されたアクセス特権の種類とは無関係に、組織全体を通して常に１個だけであることを保証するため、アクセス制御マネージメントが効率的に実行される。

【００１４】本発明の更に別の局面によれば、保護文書のフォーマットは、文書のセキュリティ情報が常に保護対象の文書に付随するように設計される。この一体化機構によって、保護文書に含まれるセキュリティ情報を失うことなく、保護文書を別の場所へ移すことが容易になり、他の場所から保護文書にアクセスすることが困難になる。一実施例によれば、保護ファイル若しくは保護文書は、ヘッダと称される添付部と、暗号文書若しくは暗号データ部の二つの部分を含む。ヘッダは、アクセス規則及びファイル鍵を指定するか、若しくは、収容するセキュリティ情報を含む。アクセス規則は、保護文書への制限的アクセスが容易に実現できるようにさせ、本質的に保護文書にアクセスすることができる人、時間、方法、場所を決定する。ファイル鍵は、暗号データ部を暗号化／復号化するため使用される。適当なアクセス特権を与えられた人だけが、暗号データ部の暗号化／復号化のためファイル鍵の取得を許可される。実施形態の精密さに応じて、ヘッダは、文書のセキュリティ種類が容易に検出できるように他の情報（例えば、フラグ、署名、若しくは、バージョン番号）を収容するようにしてもよい。或いは、暗号セキュリティ情報と、暗号データ部の二つの部分は、保護ファイル若しくは保護文書の形にするためもう一度暗号化してもよい。

【００１５】本発明の更に別の局面によれば、クライアント装置で実行可能なクライアント・モジュールは、ローカル記憶場所、別のコンピュータ機械、若しくは、データネットワーク上のどこかの場所に置かれた保護文書へのアクセス制御を行うように構成される。一実施例によれば、クライアント・モジュールは、オペレーティングシステムで動作するように組み込まれた文書保護用モジュールを含む。特に、文書保護用モジュールは、アクセスされる文書が通過するパスで動作するので、文書は、セキュリティ種類を検査又は検出される。文書が保護されているとき、文書保護用モジュールは、アクセス規則に関する文書のヘッダ内のセキュリティ情報を復号するためユーザ鍵若しくはグループ鍵を取得する。文書にアクセスするユーザが保護文書に対するアクセス特権を付与されていると判定された場合、ファイル鍵が保護情報から取得され、暗号モジュールが作動され、ファイル鍵で暗号データ部を復号化する。同様に、文書を保護する必要がある場合、暗号モジュールは、暗号データ部を作成するため、文書からのクリアデータを暗号化する。文書保護用モジュールは、保護文書を生成するため、適当な、或いは、望ましいセキュリティ情報を、暗号データ部と一体化する。文書保護用モジュールはオペレーティングシステムで動作するので、暗号プロセス／復号プロセスは、ユーザに気付かれない。

【００１６】本発明の更に別の局面によれば、クライアント装置のクライアント・モジュールは、ネットワークから離れているユーザに、オフラインアクセス機構を提供するためオフラインアクセスモジュールを作動させる。ユーザがネットワーク環境から離れることを決めたとき、又は、ユーザが出張中のとき、オフラインアクセス要求が、クライアント装置のオフラインアクセスモジュールによって作成され、アクセス制御サーバへ転送される。これに応答して、アクセス制御サーバは、ユーザ、並びに、ユーザが保護文書にオフラインでアクセスするためのクライアント装置にオフラインアクセス要求を許可する。一実施例によれば、アクセス制御サーバは、所定の時間が経過すると自動的に有効期限が切れるか、或いは、次の機会にクライアント装置がアクセス制御サーバへ接続するときに無効になる修正された若しくは一時的なアクセス規則、アクセス特権、又は、ユーザ鍵を供給する。その結果として、ユーザは、クライアント装置内の一部若しくは全部の保護文書にアクセスすることができ、同時に、保護文書を作成することも可能であり、これらの保護文書は、一時的なアクセス規則、アクセス特権若しくはユーザ鍵でアクセスするか、若しくは、保護される。オフラインアクセス期間中に、アクセス報告マネージャが保護文書にアクセスするユーザの全ての活動を記録するため作動される。クライアント装置がアクセス制御サーバに再接続されたとき、アクセス制御マネージメントと、オフラインでアクセスされた保護文書若しくは作成された保護文書の同期が容易に実現されるように、保護文書のアクセス活動記録がアクセス制御サーバへ通知される。

【００１７】本発明のその他の目的、特徴及び効果は、本発明の実施例の詳細な記述を、添付図面を参考にして、検討することによって明白になるであろう。

【００１８】
【発明の実施の形態】本発明の上記及びその他の特徴、局面及び利点は、以下の記述、特許請求の範囲に記載された事項、並びに、添付図面に関してよりよく理解されるであろう。
【００１９】本発明は、デジタル資産に対して常にパーベイシブ・セキュリティを提供する方法、システム、アーキテクチャ及びソフトウェア製品（プログラム）に関する。一般的に、パーベイシブ・セキュリティとは、デジタル資産が常に保護され、適当なアクセス特権を与えられた認証されたユーザだけがアクセスすることができることを意味する。本発明は、特に、企業環境に適している。
【００２０】以下の説明では、多数の特定の細部が本発明の完全な理解を助けるために記載されている。しかし、当業者には明らかであるように、本発明は、このような特定の細部を用いなくても実施できる。本明細書における記述及び表現は、自分の業績を他の当業者に最も効率的に伝えるため、熟練者若しくは当業者によって使用される一般的な手段である。別の例では、周知の方法、手続、コンポーネント及び回路は、本発明の局面を不必要に分かり難くすることを避けるため詳細には記述されていない。
【００２１】「一実施例」或いは「（ある）実施例」という言葉は、その実施例に関して記述された特定の特徴、構造若しくは特性が本発明の少なくとも一つの実施例に含まれることを意味する。明細書の様々な場面に「一実施例において（一実施例によれば）」という句が使用されているが、これらが全て同じ実施例を指定しなければならないものではなく、相互に独立した別個又は代替的な実施例を指定しなければならない訳でもない。更に、処理フローチャートにおけるステップの順序、或いは、本発明の一つ以上の実施例を表現する図は、本質的に何ら特定の順序を指定するものではなく、本発明における何らかの限定を意味するものでもない。
【００２２】本発明の記述を容易にするため、以下の記述を通じて使用されるある種の用語を定義しておくことが必要であろう。以下の定義は、一実施例に従って本発明の理解を助け、本発明を記述するためのものであることに注意する必要がある。これらの定義は、実施例の観点からある種の制限を含むように思われるかもしれないが、当業者には明らかであるように、これらの用語の実際の意味はこのような実施例に限定されることなく広く適用可能である。
【００２３】〔デジタル資産〕デジタル資産は、様々なタイプの文書、マルチメディアファイル、ストリーミングデータ、動的若しくは静的データ、実行可能コード、画像、並びに、テキストを含む電子データのタイプを定義するが、これらの例に限定されるものではない。
【００２４】〔ファイル〕又は〔文書〕ファイル又は文書は、互換的に使用されているが、あるタイプのデジタル資産を示し、一般的に、クリアモードであり、すなわち、事前知識が無くても一つ以上のアプリケーションからアクセスすることが可能である。ここで、ファイル又は文書のアクセスは、ファイル又は文書のアクセスを要求したユーザによって望まれるフォーマット又は結果で、ファイル又は文書を、開く、閲覧する、編集する、再生する、聴く、印刷するための要求である。
【００２５】〔保護ファイル〕又は〔保護文書〕保護ファイル又は保護文書は、事前知識無しではアクセスすることができないタイプのデジタル資産を定義する。事前知識の一例には、パスワード、秘密フレーズ、生物測定（バイオメトリック）情報、或いは、１個以上の鍵などが含まれるが、これらの例に限定されない。
【００２６】〔暗号ファイル〕又は〔暗号文書〕暗号ファイル又は暗号文書は、暗号（すなわち、暗号手法の導入）によって暗号化されたファイル又は文書を表す。
【００２７】〔ファイル鍵〕ファイル鍵は、暗号鍵とも呼ばれる事前知識の一例であり、一旦獲得されると、暗号文書を解読又は復号化するため使用される。
【００２８】〔ユーザ鍵〕ユーザ鍵は、ユーザ若しくはユーザのグループと関連した、又は、ユーザ若しくはユーザのグループを識別する別の暗号鍵であり、ファイル鍵を獲得するため使用される。保護ファイルのあるフォーマットによれば、ユーザ鍵はファイル鍵を獲得するため使用され、次に、ファイル鍵は、暗号文書を解読若しくは復号化し、別のユーザ鍵又は同一のユーザ鍵がファイル鍵を秘密にするため、或いは、暗号化するため使用される。
【００２９】〔アクセス特権〕アクセス特権は、保護ファイル若しくは保護文書に関してユーザに与えられた一つ以上の権利である。ユーザは、そのユーザのアクセス特権によって制限されている場合、特定の期間中に指定された場所からしか保護ファイルにアクセスすることができない。オプションとして、アクセス特権は、ユーザがログインした特定のホスト、ファイル転送プロトコル、アクセスアプリケーション（モデル及び／又はバージョン）、アクセス特権を他者（例えば、コンサルタント）に与える許可、或いは、他のグループの会員資格などに別の制限を指定することがある。
【００３０】〔アクセス規則〕アクセス規則は、ユーザが保護ファイル又は保護文書に行う処置を制限するためのフラグ又は指定された許可である。本発明の一実施例によれば、アクセス規則の少なくとも一部分は、保護ファイル又は保護文書に収容される。一部のケースでは、アクセス規則は、適当なアクセス特権が与えられたユーザによって拡張可能である。
【００３１】〔クライアント装置、コンピュータ、若しくは、マシーン〕クライアント装置、コンピュータ、若しくは、マシーンは、互換的に使用され、典型的に保護

文書にアクセスするユーザによって使用される端末装置である。

【００３２】〔サーバ装置、コンピュータ、若しくは、マシーン〕サーバ装置、コンピュータ、若しくは、マシーンは、互換的に使用され、コンピュータ装置を表す。一実施例によれば、このようなコンピュータ装置は、クライアント・マシーン又はユーザからアクセス可能である保護文書に対するアクセス制御（ＡＣ）マネージメントを行う。

【００３３】〔クライアント・モジュール〕クライアント・モジュールは、一般的に、本発明の一実施例の実行可能バージョンを表し、典型的に、本発明において熟考された機能、特徴、利益、及び、効果を実現するため、クライアント装置にロードされる。

【００３４】〔サーバ・モジュール〕サーバ・モジュールは、一般的に、本発明の一実施例の実行可能バージョンを表し、典型的に、本発明において熟考された機能、特徴、利益、及び、効果を実現するため、サーバ装置にロードされる。

【００３５】〔サーバ及びクライアント〕特に断らない限り、或いは、明示しない限り、サーバは、サーバ装置若しくはサーバ・モジュールを示し、クライアントは、クライアント装置若しくはクライアント・モジュールを示し、何れの場合も、特定の意味は文脈から明白である。

【００３６】以下、図１Ａ乃至７Ｃを参照して、本発明の実施例を説明する。しかし、当業者は、本発明がこれらの実施例によって制限されないので、これらの図面に関する詳細な記述は例示の目的であることが容易に分かるであろう。

【００３７】図１Ａは、本発明の一実施例によって本発明が実施される基本システムの構成図である。製品説明書、顧客リスト、及び、価格スケジュールのような文書又はファイルは、クライアント・コンピュータ１００で実行されるオーサリングツールを使用して作成される。クライアント・コンピュータは、デスクトップ型コンピュータ装置、ラップトップ型コンピュータ、或いは、携帯型コンピューティング装置である。オーサリングツールの例には、Microsoft Office（登録商標）（例えば、Microsoft Word（登録商標）、Microsoft PowerPoint（登録商標）、及び、Microsoft Excel（登録商標））、Adobe FrameMaker（登録商標）、並びに、Adobe Photoshop（登録商標）が含まれる。

【００３８】一実施例によれば、クライアント・コンピュータ１００には、本発明の一実施例のリンク及びコンパイルされたバーション、又は、インタープリットされたバーションであるクライアント・モジュールがロードされ、クライアント・コンピュータ１００は、データネットワーク（すなわち、インターネット若しくはローカル・エリア・ネットワーク）を解してサーバ１０４若しくは１０６と通信する機能を備えている。別の実施例によれば、クライアント・コンピュータ１００は、私設リンクを経由してサーバ１０４に接続される。後述するように、オーサリングツールによって作成された文書は、詳述されるクライアント・モジュールによって保護処理される。クライアント・モジュールは、実行されると、保護文書が記憶装置（例えば、ハードディスク若しくはその他のデータリポジトリ（保管場所））で常に保護されることを保証するように構成される。本発明によれば、文書は、保護モードで保存され、適当なアクセス特権が与えられたユーザだけによってアクセスされる。一般的に、ユーザのアクセス特権には、閲覧許可、コピー許可、印刷許可、編集許可、転送許可、アップロード／ダウンロード許可、及び、ロケーション（場所）許可が含まれるが、これらの例に限定されるわけではない。

【００３９】一実施例によれば、作成文書は、好ましくは、ユーザに気付かれること無く、暗号化処理を受ける。換言すると、作成文書は、オーサリングアプリケーションの下で暗号化若しくは復号化されるので、ユーザはこの処理に気付かない。暗号文書を復号化するためのファイル鍵を獲得するための鍵（以下では、ユーザ鍵と称される）は、アクセス特権と関連づけられる。適当なアクセス特権を付与されたユーザだけが保護文書にアクセスすることができる。

【００４０】ある場面では、保護文書は、ネットワーク１１０を介して、中央リポジトリとしての役割を担うコンピュータ装置若しくは記憶装置１０２にアップロードされる。必須ではないが、ネットワーク１１０は、好ましくは、コンピュータ１００とコンピュータ装置１０２の間に私設リンクを設定する。このようなリンクは、企業の内部ネットワークによって、又は、インターネット経由の保護通信プロトコル（例えば、ＶＰＮ及びＨＴＴＰＳ）によって実現される。或いは、このようなリンクは、ＴＣＰ／ＩＰリンクによって簡単に実現してもよい。このようにして、コンピュータ１００上の保護文書は遠隔的にアクセスされる。

【００４１】別の場面では、コンピュータ１００と、コンピュータ装置若しくは記憶装置１０２は、分離不能であり、この場合、コンピュータ装置若しくは記憶装置１０２は、保護文書を保持するか、又は、保護ネットワークリソース（例えば、動的ウェブコンテンツ、データベース問い合わせの結果、或いは、ライブのマルチメディア入力）を取得するローカル記憶装置でもよい。保護文書若しくは保護ソースが実際に存在する場所とは無関係に、適当なアクセス特権を与えられたユーザは、アプリケーション（例えば、Internet Explorer（登録商標）、Microsoft Word（登録商標）、又は、Acrobat Reader（登録商標））を使用して、コンピュータ１００又は装置１０２から保護文書若しくは保護ソースにアクセスすることができる。

【００４２】サーバ装置１０４は、ローカル・サーバと呼ばれる場合もあり、ネットワーク１０８とネットワーク１１０の間に接続されたコンピュータ装置である。一実施例によれば、サーバ１０４は、本発明の一実施例のコンパイル、リンクされたバージョンのサーバ・モジュールのローカルバージョンである。後述するように、ローカルバージョンは、指定されたユーザ若しくはクライアント・コンピュータのグループ、又は、ロケーションにサービスを提供するように構成された局在化されたサーバ・モジュールである。別のサーバ装置１０６は、中央サーバとも呼ばれ、ネットワーク１０８に接続されたコンピュータ装置である。サーバ１０６は、サーバ・モジュールを実行し、集中アクセス制御（ＡＣ）マネージメントを組織全体若しくはビジネス全体に提供する。従って、ローカル・サーバ内の夫々のローカル・モジュールは、中央サーバと協調して、分散型アクセス制御マネージメントを行う分散機構を形成する。このような分散型アクセス制御マネージメントは、企業全体又はビジネスロケーションに対して中央サーバによって行われる集中アクセス制御マネージメントの信頼性、確実性及び拡張性を保証する。後述するように、中央サーバのサーバ・モジュールは、データベースを保持するか、又は、データベースと連結し、このデータベースは、ユーザと、ユーザに対応した組織全体若しくはビジネスに関するアクセス特権のリストと、フォルダ若しくはファイルのための規則と、を収容するが、これらの例に限定されるものではない。一方、ローカル・モジュールは、データベースの一部若しくは全体を保持するか、若しくは、連結するように構成され、ローカル・サーバの近くのユーザのグループにサービスを行う。

【００４３】図１Ｂは、中央サーバ及びローカル・サーバが利用されるシステムの構成図である。この構成は、多数の地理的なロケーション若しくはオフィスを有する大企業に対応する。中央サーバ１０６は、企業全体のアクセス特権及びアクセス規則を管理するデータベースを保持する。この構成の一つの特徴は、大規模なユーザのグループに耐故障性（フォールト・トレランス）と、効率的なアクセス制御マネージメントを提供することである。一箇所（単一ロケーション）でユーザの各々に対するアクセス制御を実行する中央サーバ１０６を設けるのではなく、多数のローカル・サーバ１０４（例えば、１０４－Ａ、１０４－Ｂ、・・・及び１０４－Ｎ）が、個別のロケーション若しくはオフィスにサービスを行うため分散形式で利用される。各ローカル・サーバ１０４は、各ローカル・サーバ１０４の近くのユーザを管理するため、中央サーバ１０６で実行中のサーバ・モジュールから取得若しくは複製されたローカル・モジュールを実行する。中央サーバ１０６は、ユーザを管理するだけではなく、必要に応じて、アクセス制御管理を集中化する。

【００４４】一実施例によれば、ローカル・モジュールは、少数のロケーション若しくはユーザのグループのために効率的に動くサーバ・モジュールのカスタムバージョンである。例えば、ローカル・サーバ１０４－Ａは、ロケーションＡのユーザ若しくはコンピュータ１０２－Ａのためだけの機能を果たし、ローカル・サーバ１０４－Ｂは、ロケーションＢのユーザ若しくはコンピュータ１０２－Ｂのためだけの機能を果たす。その結果として、中央サーバ１０６がメンテナンスのため停止されるとき、或いは、ユーザが保護文書にアクセスする必要があるときに作動していなくても、アクセス制御は支障を来たさない。中央サーバ１０６と協調したローカル・サーバ１０４の詳細動作は後述する。

【００４５】他の実施例によれば、ローカル・モジュールは、サーバ・モジュールの複製バージョンであり、接続されたとき（例えば、定期的に、若しくは、要求に応じて）、サーバ・モジュールと最新情報を交換する。実現形態に応じて、サーバ・モジュールの一部又は全部が、ユーザ若しくはクライアント装置との通信が効率的であり、かつ、耐故障性があることを保証するため、ローカル・サーバに複製される。その結果として、中央サーバ１０６がメンテナンスのため停止されるとき、或いは、ユーザが保護文書にアクセスする必要があるときに作動していなくても、アクセス制御は支障を来たさない。例えば、このような状況において、任意のローカル・サーバ１０４は、準備をして、中央サーバの代わりに使用される。中央サーバ１０６が動いているとき、或いは、ローカル・サーバ１０４と通信しているとき、夫々のローカル・サーバで、ユーザ若しくはユーザの活動に関して収集された情報は、中央サーバ１０６へ返信される。この点に関して、中央サーバ１０６と協調したローカル・サーバ１０４の詳細動作は後述される。

【００４６】図１Ｃは、小規模のユーザのグループに適してシステムの構成図である。この構成の場合、ローカル・サーバは利用されない。サーバ・コンピュータ１１２は、サーバ・モジュールがロードされ、各ユーザ若しくは各端末コンピュータ１１６（１台だけが図示されている）には、クライアント・モジュールがロードされる。その結果として、サーバ・コンピュータ１１２は、ユーザ毎に、或いは、端末コンピュータ１１６毎にアクセス制御を実行する。

【００４７】小規模のユーザのグループと大規模のユーザのグループとの間には、ユーザ数に関する限り、明確な区別が無い点に注意する必要がある。以下の説明によって、当業者は、１台以上の別のコンピュータ装置の間でアクセス制御マネージメントを分散若しくはバランスさせる方法を理解するであろう。以下の本発明の説明を容易に行うため、図１Ｂに示された場面を想定する。当業者は、以下の説明が図１Ｃに、並びに、１台以上の中央サーバと１台以上のローカル・サーバとの間で考えら

れる他の場面の方が望ましい状況にも同じように適用可能であることを理解するであろう。

【００４８】図１Ｄは、本発明の一実施例が組み込まれ、実行されるコンピュータ装置の内部構成のブロック図である。装置１１８は、クライアント装置（例えば、図１Ａ及び１Ｂにおけるコンピュータ１００、１０２、或いは、図１Ｃにおけるコンピュータ１１６）、又は、サーバ装置（例えば、図１Ａ及び１Ｂにおけるサーバ１０４、１０６、或いは、図１Ｃにおけるサーバ１１２）に対応する。図１Ｄに示されるように、装置１１８は、データバス１２０及び装置インタフェース１２４と接続された中央処理ユニット（ＣＰＵ）１２２を含む。ＣＰＵ１２２は、データを処理し、おそらく、同期的動作のためデータバス１２０に接続された全ての装置及びインタフェースを管理する命令を実行する。実行される命令は、例えば、ドライバ、オペレーティングシステム、ユーティリティ、若しくは、アプリケーションに関係がある。装置インタフェース１２４は、図１Ａのコンピュータ装置１０２のような外部装置に接続され、外部装置からの保護文書を、データバス１２０を介して、メモリ１３２若しくは記憶装置１３６に取り込む。データバス１２０には、ディスプレイ・インタフェース１２６、ネットワーク・インタフェース１２８、プリンタ・インタフェース１３０及びフレキシブルディスクドライブ・インタフェース１３８が接続される。一般的に、本発明の一実施例の実行可能バージョンのクライアント・モジュール、ローカル・モジュール又はサーバ・モジュールは、フレキシブルディスクドライブ・インタフェース１３８、ネットワーク・インタフェース１２８、装置インタフェース１２４、又は、データバス１２０に接続されたその他のインタフェースを介して、記憶装置１３６に保存される。ＣＰＵ１２２がこのようなモジュールを実行することによって、コンピュータ装置１１８は、本発明において望まれるように動作する。一実施例において、装置インタフェース１２４は、コンピュータ装置１１８のユーザの認証を容易に行うため、キャプチャー装置１２５（例えば、指紋センサ、スマートカードリーダ、又は、音声レコーダ）と通信するためのインタフェースを提供する。

【００４９】ランダムアクセスメモリ（ＲＡＭ）のようなメインメモリ１３２は、ＣＰＵ１２２に命令と、データ及びその他の命令用の記憶装置１３６へのアクセスを与えるため、データバス１２０に接続される。特に、本発明における文書保護用モジュールのような蓄積されたアプリケーションプログラム命令を実行するとき、ＣＰＵ１２２は、本発明によって熟考された結果を達成するためデータを操作する。読み出し専用メモリ（ＲＯＭ）１３４は、もしあるとすれば、キーボード１４０、ディスプレイ１２６及び印刷装置１４２の動作用の基本入力／出力動作システム（ＢＩＯＳ）のような実行可能命令を保持するため設けられる。

【００５０】図２Ａを参照するに、作成文書２００の保護処理の一例が示されている。文書がアプリケーション若しくはオーサリングツール（例えば、Microsoft WORD（登録商標））を用いて作成された後、「保存（ＳＡＶＥ）」、「名前を付けて保存（ＳＡＶＥ　ＡＳ）」、若しくは、「閉じる（ＣＬＯＳＥ）」のようなコマンドの作動時に、若しくは、オペレーティングシステム、アプリケーション自体、若しくは、サーバを用いて予め登録されたアプリケーションによって呼び出される自動保存時に、作成文書２００に保護処理２０１が施される。保護処理２０１は、暗号処理２０２から始まり、すなわち、作成された、若しくは、記憶装置に書き込まれた文書２００は、ファイル鍵を用いて暗号部によって暗号化される。換言すると、暗号文書は、ファイル鍵（すなわち、暗号鍵）を用いなければ開くことができない。

【００５１】文書２００のためのアクセス規則２０４の組が取得され、ヘッダ２０６と関連付けられる。一般的に、アクセス規則２０４は、保護処理後の文書２００にアクセスできる人、及び／又は、アクセスする方法を決定するか、或いは、調整する。ある種のケースでは、アクセス規則２０４は、文書２００にアクセスすることができる時間又は場所を決定、或いは、調整する。典型的に、ヘッダは、サイズの小さいファイル構造であり、得られた保護文書に関するセキュリティ情報を格納するか、或いは、おそらく、セキュリティ情報にリンクされる。厳密な実施形態に応じて、セキュリティ情報は、ヘッダに完全に収容されたり、或いは、ヘッダに含まれるポインタによって指定されたりする。一実施例によれば、アクセス規則２０４は、セキュリティ情報の一部として、ヘッダ２０６に収容される。セキュリティ情報は、ファイル鍵を更に含み、ある種のケースでは、このようなアクセスが許可されたユーザによって要求された場合には、オフラインアクセス許可（例えば、アクセス規則にある）を含む。セキュリティ情報は、暗号セキュリティ情報２１０を生成するため、許可されたユーザに関連したユーザ鍵を用いて暗号技術によって暗号化される。暗号ヘッダは、その他の情報が追加されていない場合には、保護文書２０８を作成するため、暗号文書２１２に添付される。

【００５２】尚、暗号技術は、多数の暗号／復号方式のうちの一つに基づいて実施される。このような暗号方式の例には、データ暗号化規格（ＤＥＳ）、ブロウフィッシュ・ブロック暗号、及び、ツーフィッシュ暗号が含まれるが、これらの例に限定されない。従って、本発明の動作は、これらの普及した暗号／復号方式の選択範囲に限定されない。効率的で信頼性の高い任意の暗号／復号方式を使用することができる。そのため、暗号／復号方式の細部については、本発明の局面を分かり難くすることを避けるため、これ以上説明しない。

【００５３】本質的に、保護文書２０８は、文書自体と、文書に対応したセキュリティ情報の二つの部分を含み、両者は暗号形式である。文書にアクセスするためには、文書を暗号化するいため使用されるファイル鍵を取得する必要がある。このファイル鍵は暗号セキュリティ情報に含まれている。ファイル鍵を取得するため、ユーザ若しくはグループ鍵を取得し、アクセス試験に通過するための認証を受ける必要がある。アクセス試験では、セキュリティ情報中のアクセス規則がユーザのアクセス特権と比較される。

【００５４】一実施例によれば、アクセス規則を含む暗号セキュリティ情報、又は、ヘッダは、保護特性又は保護文書の早期検出が容易に行われるように、暗号文書（データ部）の先頭に配置される。このような配置の一つの零点は、アクセスアプリケーション（すなわち、オーサリング又はビューイングツール）がヘッダを復号化するため文書保護用モジュールを直ちに作動できることである。認証済みのユーザ鍵を用いたヘッダの復号化に成功した後、アクセス規則は、ユーザのアクセス特権と比較される。保護文書を要求したユーザが適当なアクセス特権を保有している場合、文書のクリアコンテンツ（暗号化されていない内容）がアクセスアプリケーションにロードされ、ユーザがアクセス特権を保有していない場合、拒絶中値（例えば、メッセージ若しくは空白文書）がユーザへ送信される。しかし、暗号セキュリティ情報又はヘッダは、暗号文書のどの場所に配置してもよく、暗号データ部に連続的に埋め込まれない場合もある。本発明によれば、暗号ヘッダは、常に、暗号データ部に添付され、すなわち、セキュリティ情報は保護された文書と一体化されている。この一体化機構によって、保護文書に含まれるセキュリティ情報を失うことなく、保護文書を他のロケーションへ容易に転送できるようになる。

【００５５】本発明における一つの特徴は、保護されている文書がユーザに気付かれないことである。換言すると、保護文書若しくは保護ファイルは、保護される前のファイルと同じファイル拡張子をもつように構成されているので、ファイルにアクセスするため指定されたアプリケーションは保護ファイルにアクセスするため実行され得る。例えば、新しく作成されたワード文書ｘｙｚ．ｄｏｃは、アプリケーションＷＩＮＷＯＲＤ．ＥＸＥによってアクセスすることができる。ワード文書に保護処理が行われた後、保護文書は同じファイル名、すなわち、ｘｙｚ．ｄｏｃのままの状態に保たれ、そのワード文書のアクセス規則がユーザに文書を開くことを許可していないため、アプリケーションが文書を開くことに失敗する場合を除いて、同じアプリケーションＷＩＮＷＯＲＤ．ＥＸＥでこのワード文書にアクセス可能である。

【００５６】或いは、フォルダ内の保護文書は、実質的に、通常の文書と同じように見え、アプリケーションがその文書の内容にアクセスできない場合を除いて、この文書が作動状態にされたときに同じアプリケーションを始動する。例えば、保護文書のアイコン若しくはファイル名は、保護されていない文書と区別するため、別の色、或いは、視覚的な標識付きで現れる。保護文書が装置若しくは読み取り可能媒体（例えば、ＣＤ若しくはディスク）内で無意図的に終了したとき、読み取り可能な媒体を読むための装置のユーザ、又は、装置に適当なユーザ鍵が与えられていない場合、或いは、ユーザをできなかった場合、保護文書のアクセスは成功しないであろう。

【００５７】尚、保護文書のヘッダは、本発明の原理から逸脱することなく、上述の少数のフォーマットとは別のフォーマットで構成することも可能である。例えば、保護文書は、複数の暗号ヘッダを含むヘッダを収容し、各暗号ヘッダは、一人の指定されたユーザ、又は、グループユーザだけのアクセスが許可される。或いは、保護文書のヘッダは、セキュリティ情報の２個以上の組を含み、各組は、一人の指定されたユーザ若しくはユーザのグループのためのものであり、単一のファイル鍵が全ての組で使用される。アクセス規則の一部若しくは全部は、保護文書にアクセスすることができるユーザによって閲覧され、或いは、更新される。

【００５８】後述するように、保護文書にアクセスするため、ユーザは、暗号セキュリティ情報若しくはヘッダを最初に復号化するユーザ鍵が必要である。一実施例において、ユーザ鍵は、ローカル・サーバ又は中央サーバへのユーザのログインと関連付けられる。ユーザと関連した適当なアクセス特権は、ユーザが認証されたとき、サーバで予め登録され、適切にログインしたときに、有効とされる。許可又はアクセス特権に応じて、保護文書内のアクセス規則は、文書の内容をユーザに公開してもよいかどうかを決定する。

【００５９】一実施例によれば、アクセス規則は、ＨＴＭＬやＳＧＭＬのようなマークアップ言語で表される。好ましい一実施例では、マークアップ言語は、本質的に情報アクセスのポリシーを表現するためのＸＭＬ仕様である拡張可能アクセス制御マークアップ言語（ＸＡＣＭＬ）である。一般的に、ＸＡＣＭＬは、許可された動作の精細な制御と、アクセス要求元の特性の影響と、要求が行われたプロトコルと、動作のクラスに基づく認証と、内容の内省（すなわち、要求元と、属性値がポリシー作成者に知られていないターゲット内の属性値の両方に基づく認証）とを扱うことができる。その上、ＸＡＣＭＬは、認証機構の導入者をガイドするため、ポリシー認証モデルを提案することが可能である。

【００６０】次に、ＸＡＣＭＬで表現されたアクセス規則の例を示す：

```
〈rule〉
  〈doc_type〉
        PDF
  〈/doc_type〉
  〈grantor name="ACCTG"/〉
  〈grantee name="MKTG"/〉
  〈grantee name="PR"/〉
  〈action〉
        VIEW
  〈/action〉
  〈action〉
        PRINT
  〈/action〉
  〈conditions〉
  〈delivery_channels〉
  〈min_time_day〉
        2700
  〈/min_time_day〉
  〈expiry_date〉
        3 Aug, 2002年12月9日
  〈/expiry_date〉
  〈/conditions〉
〈/rule〉
```

【００６１】上記例の意味を言葉で表現すると、「ＡＣＣＴＧ（会計グループ）によって作成された新しいＰＤＦ文書は、ＨＴＴＰ経由でダウンロードされ、２００２年８月３日以前の毎日午後５時までにアクセスするという条件で、ＭＫＴＧ（マーケッティンググループ）及びＰＲ（渉外グループ）による閲覧及び印刷が許可される。」になる。

【００６２】図２Ｂは、ヘッダ２２２及び暗号部２２４を含む保護文書の例示的な構造の説明図である。ヘッダ２２２は、暗号文書２２４へのアクセスを本質的に制御する暗号セキュリティ情報を収容したセキュリティ情報ブロック２２６を含む。ある種の実現形態では、ヘッダ２２２は、文書２２０が保護されていることを示すため、フラグ２２７（例えば、所定のデータの組）を含む。セキュリティ情報ブロック２２６は、一つ以上のユーザＩＤ２２８と、アクセス規則２２９と、少なくとも一つのファイル鍵２３０と、その他の情報２３１と、を格納する。ユーザＩＤ２２８は、ファイル鍵２３０が取得される前にアクセス規則２２９に対して比較（照合）された許可されたユーザのリストを維持する。アクセス規則２２９は、少なくとも暗号文書２２４にアクセスすることができる人と方法を決定する。実施形態に依存して、他の情報２３１が、暗号文書２２４へのセキュア・アクセスを容易に行う他の情報を組み込むため使用される。この他の情報の例には、バージョン番号、若しくは、作成者識別子が含まれる。

【００６３】一般的に、文書は暗号技術（例えば、対称暗号方式若しくは非対称暗号方式）で暗号化される。暗号化とは、データを、適当な知識（例えば、鍵）を用いることなく読むことが不可能になる形式に変換することである。その目的は、たとえ、他の暗号データへのアクセス権が与えられているとしても、意図されていない他人から情報を隠したままの状態に保つことによってプライバシーを保証することである。復号化は暗号化の反対である。暗号化及び復号化は、一般的に、鍵と称される、ある種の秘密情報、の使用を必要とする。一部の暗号化方式では、暗号化と復号化の両方に同じ鍵が使用され、別の暗号化方式では、暗号化と復号化に使用される鍵は別個である。文書へのアクセスを制御する目的のため、集合的にファイル鍵と呼ばれる鍵は、暗号化と復号化に対して同一でも別個でもよく、好ましくは、ヘッダに含まれるか、若しくは、ヘッダによって指定されたセキュリティ情報に格納され、一旦取得されると、暗号文書の復号化のために使用される。

【００６４】鍵が誰にも取得されない、若しくは、誰からもアクセスできないことを保証するため、鍵自体は、アクセス特権及びアクセス規則によって守られる。文書を要求するユーザが、アクセス規則によって許可され得る適当なアクセス特権を保有する場合、鍵は暗号文書の復号化を進めるために取得される。

【００６５】セキュリティ情報又はヘッダ（フラグが組み込まれていない場合）が容易に取得できないことを保証するため、ヘッダ自体は暗号技術で暗号化される。厳密な実施態様に依存して、ヘッダ用の暗号技術は、文書用の暗号技術と同一である場合と同一ではない場合とがある。暗号ヘッダを復号化するための鍵（ユーザ鍵と称される）は、例えば、端末装置のローカル記憶装置に保存され、関連したユーザが認証された場合に限り有効な状態に（活性化）される。その結果として、許可されたユーザだけが保護文書にアクセスすることができる。

【００６６】オプションとして、二つの暗号部（すなわち、暗号ヘッダと暗号文書）は、再暗号化され、ユーザ鍵でしか復号化できない。別のオプションとして、暗号部（一方若しくは全部）は、暗号部又は保護文書２２０にエラーが生じていないことを保証するため、巡回冗長検査を使用するようなエラーチェック用部２２５によってエラーチェックされる。

【００６７】図２Ｃ．１は、ヘッダ２３８及び暗号部２３９を含む保護文書２３６の典型的な構造の説明図である。ヘッダ２３８は、４種類のエンティティ２４０～２４３が保護文書２３６にアクセスすることを許可する。４種類のエンティティ２４０～２４３は、二人の個人ユーザと、二つのグループユーザを含み、ここで、グループユーザとは、グループ内の全ての人が同じ特権で文書にアクセス可能であることを意味する。二人の個人ユーザは、二つの別々のアクセス特権を与えられる。ユーザＡは文書を読むことだけが許可され、ユーザＤは文書の

編集と読み取りが許可される。一方、グループＢの全員は文書の編集と読み取りが許可され、グループＣの全員は文書の印刷しか許可されていない。各エンティティは、対応したＩＤをもち、ＩＤは、対応したユーザ及びその固有のアクセス規則と関連付けられる。一実施例によれば、保護文書２３６のヘッダ２３８は、対応した４個のサブヘッダ２４０～２４３に分割され、各サブヘッダは、一人のユーザ若しくは一つのグループに割当てられ、ファイル鍵を収容し、別個のユーザ鍵で暗号化される。換言すると、ユーザＡが保護文書２３６を要求するとき、ユーザＡに指定されたヘッダ２４０だけが、ユーザＡに属し、ユーザＡで認証されたユーザ鍵（例えば、鍵Ａ）で復号化され、残りのサブヘッダ２４１～２４３は暗号化されたままの状態で保たれる。いずれにしても、サブヘッダ２４１～２４３のうちの１個が復号化された後、保護文書は、復号サブヘッダから取得された鍵（例えば、ファイル鍵）で復号化される。

【００６８】図２Ｃ．２は、ヘッダ２５２及び暗号部２５４を含む保護文書２５０の別の構造の例の説明図である。ヘッダ２５２は、ユーザブロック２５６及び規則ブロック２５８を更に含む。ユーザブロック２５６は、クリア部及び暗号部２６０を含む。クリア部は、ユーザ／グループＩＤ及びブロックバージョン番号を含む。暗号部２６０は、暗号に応じたユーザ鍵で暗号化される。異なり得るアクセス特権が与えられた別々のグループ／ユーザの数がＮである場合、Ｎ個の暗号部が存在し、各暗号部は、対応したユーザ鍵で暗号化される。暗号部２６０は、特に、取得された後に暗号データ部２５４を復号化するため使用することができるファイル鍵を収容する。更に、暗号部２６０は、暗号部２５４の暗号化／復号化を促進するための暗号情報を含む。

【００６９】規則ブロック２５８は、最終的にユーザブロック２５６に保持されるファイル鍵を使用して、個別に、又は、暗号文書２５４と共に、暗号化することができる。規則ブロック２５８を暗号化するため、個別のユーザ鍵ではなく、ファイル鍵を使用する利点は、全ての許可されたユーザ／グループに誰がどのようなアクセス規則及び権利を保有するかを閲覧させることができる機構を提供することである。一実施例によれば、規則ブロック２５８に対する攻撃を阻止するため、乱数、又は、初期化処理からの結果（例えば、ベクトル）が規則ブロック２５８の先頭に追加される。

【００７０】図２Ｃ．３は、図２Ｃ．２の保護文書構造のヘッダに対応したヘッダ２６６の例の説明図である。ヘッダ２６６は、セグメント数を含む。クリアモードのこれらのセグメントの他に、セグメント２６７～２６９は暗号化される。特に、保護ファイルは、マーケッティンググループとエンジニアリンググループの二つのグループからアクセスできるように構成される。二つのグループの全ユーザは、認証されたユーザ鍵を用いてファイルにアクセスすることが可能であると考えられる。一実施例によれば、セグメント２６７は、特に、マーケッティングユーザに指定されたユーザ鍵を用いて暗号化され、セグメント２６８は、特に、エンジニアリングに指定されたユーザ鍵で暗号化される。しかし、セグメント２６７とセグメント２６８は、どちらも単一のユーザ鍵で暗号化することが可能である。何れにしても、ヘッダ２６６の暗号セグメントは、使用される暗号技術に関する対応した暗号情報に加えてファイル鍵２７０を含む。

【００７１】規則ブロック（すなわち、セグメント）２６９は、２組のアクセス規則２７１及び２７２を含む（規則の詳細は図示せず）。二つのユーザグループの各ユーザグループに一方のアクセス規則の組が対応する。規則ブロック２６９は、使用される暗号技術に応じて、ファイル鍵２７０、又は、その他の鍵のような鍵を用いて暗号化される。一実施例によれば、ユーザブロック２６７及び２６８の暗号セグメントのうちの一つは、ファイル鍵２７０を取得するため、認証されたユーザ鍵で復号化される。ファイル鍵２７０が暗号データ部の復号化に適用される前に、規則ブロック２６９はファイル鍵２７０で復号化される。アクセス規則は、次に、ユーザのアクセス特権と比較される。ユーザが保護文書へのアクセスを許可されていない場合、ファイル鍵は暗号データ部の復号化に適用されあに。ユーザが保護文書へのアクセスを許可されている場合、ファイル鍵２７０は、暗号データ部の復号化に適用される。

【００７２】図２Ｃ．１、図２Ｃ．２及び図２Ｃ．３は、保護文書の例示的な構造に過ぎないことに注意する必要がある。他の実施形態によれば、文書を復号化するために必要なファイル鍵は、単独で暗号化され、ヘッダの別個のブロックに維持される。ファイル鍵は、サブヘッダのうちの一つが復号化されたときに（ファイル鍵は維持されなくなる）、獲得可能になる。更に別の代替的な実施形態の場合、一つ以上のフラグ若しくはメッセージは、保護文書のセキュリティ情報に収容され、フラグ若しくはメッセージは、保護文書が保護されている程度を示す。例えば、保護文書は、異なるアクセスレベルを要求する通常文書、親展文書、秘密文書又は極秘文書として分類される。従って、ファイル鍵及び／又はアクセス規則に関する暗号化の多数のレベルは、許可されたユーザだけが保護文書にアクセスできることを保証するため利用される。このような説明の範囲で、他の実施形態のオプションも実現可能であり、本発明の局面を分かり難くすることを避けるため、個別には列挙しない。

【００７３】図２Ｄは、アクセス規則を設定若しくは作成するため使用できるグラフィック・ユーザ・インタフェース（ＧＵＩ）２７５の一例の説明図である。ＧＵＩ２７５は、ユーザが保護文書を片付けたとき、並びに、保護文書を指定された場所へ保存する準備ができたとき、又は、クリア文書若しくは新文書が指定された場所

へ収容される準備ができたときに作動及び／又は表示される。一実施例によれば、指定場所の全データは、実質的に類似したアクセス規則をもつ。厳密な実施形態に応じて、ＧＵＩ２７５は、指定された場所のデータにアクセスする必要のあるユーザを組み入れるため、中央サーバによって動的に生成若しくは制御される。ＧＵＩ２７５は、ユーザが課そうとしているアクセス規則の決定が容易になされるようにする。図２Ｄに示されるように、選択されたユーザのグループは、アクセスリスト２７６に加えるため選択される。アクション（動作、行動）２７７は、指定場所のデータをアクセスする方法を決定する。アクション２７７は、ＧＵＩ２７５を使用して設定してもよい。その結果として、アクセス規則を定義するパラメータは、グラフィック的に決定され、文書（例えば、ヘッダのセキュリティ情報）に組み込むためＧＵＩ２７７から集められる。一実施例において、アクセス規則は、指定されたフォルダと関連し、オプションとして暗号化された一時的ファイル（例えば、マークアップ言語フォーマット）に維持される。文書が保護ファイルとしてローカル記憶装置に書き込まれているとき、一時的ファイルは、暗号部に添付することが可能である。

【００７４】時には、ユーザは、予め定義されたアクセス規則の組をエクスポートしたり、インポートしたりする必要がある。この場合、アクセス規則を含む一時的ファイルは、エクスポートされ、段ロードされ、別の装置若しくはフォルダにインポートされる。アクセス規則のエクスポート／インポートによって、ユーザはスクラッチからアクセス規則を作成する必要がないので、ユーザにとって便利である。

【００７５】特定の場所若しくはフォルダのためのアクセス規則の組を設定する特徴の一つは、文書にアクセスする人、方法、とき、場所を指定せずに保護文書を作成するためユーザに保護用機構を与えることである。図２Ｅは、クリアフォルダ２８１と保護フォルダ２８２を含むディレクトリ構造２８０の説明図である。クリアフォルダ２８１は、一般的に、システムファイルや、保護することが意図されていないファイルを格納する。保護フォルダ２８２は、アクセスレベル毎に構成された多数のサブフォルダを含む。例えば、文書「従業員リスト」は、レベルＡのアクセス特権が与えられた全ての人によってアクセスされる。同様に、文書「製品マイルストーン」、及び、「製品仕様」若しくは「製品スケジュール」は、フォルダ２８４に対してアクセスレベルＢのアクセス特権が与えられ、フォルダ２８６に対してアクセスレベルＣのアクセス特権が与えられた人によってアクセスされる。同様に、作成文書は、フォルダ「設計チーム２」に置かれた場合、アクセスレベルＢまでのアクセス特権が与えられた人だけを許可する対応したアクセス規則を用いて自動的に暗号化される。本実施例の場合、アクセスレベルは、階層的であり、すなわち、アクセスレベルＡ認証のユーザは、アクセスＡの項目だけではなく、アクセスレベルＡの部分集合であり、アクセスレベルＡよりも低いアクセスレベルＢとＣにもアクセス可能である。

【００７６】保護されるべき文書がユーザによって始動された暗号化処理によって暗号化される従来技術のシステムとは異なり、本発明における一つの特徴は、ユーザに関する限りはユーザに気付かれないように、暗号処理（すなわち、暗号化／復号化処理）を作動させることである。換言すると、ユーザは、文書が記憶装置に書き込まれている間に暗号処理によって保護されていることに気が付かない。

【００７７】図３は、文書がユーザに気付かれないで保護されることを保証するため、文書保護用モジュール（ＤＳＭ）３０２がオペレーティングシステム３０４（例えば、WINDOWS（登録商標）2000と相互作用し、その中で動作する方法の実施態様の例の説明図である。

【００７８】アプリケーション３０６（例えば、Microsoft Word（登録商標）のようなサーバ登録アプリケーション）は、オペレーティングシステム（ＯＳ）３０４で動作し、記憶装置３０８に保持された文書にアクセスするため作動される。記憶装置３０８は、ローカル記憶場所（例えば、ハードディスク）若しくは遠隔地（例えば、別の装置）である。アクセス対象の文書のセキュリティ特性（保護、保護なし）に応じて、ＤＳＭ３０２は、暗号モジュール３１０を作動する。一実施例によれば、ＤＳＭ３０２は、原則的にオペレーティングシステムの非常に一般的な入出力命令をサポートされる装置／モジュールで理解できるメッセージに変換するデバイスドライバと多数の点で類似している。本発明が実施されるＯＳに応じて、ＤＳＭは、ＶｘＤ（仮想デバイスドライバ）、カーネル、又は、その他の適用可能なフォーマットとして実施される。暗号モジュール３１０は、ＤＳＭ３０２に収容されるか、又は、ＤＳＭ３０２によって制御され、保護文書が取り扱われるときに、動作のため作動される。

【００７９】動作中に、ユーザは、アプリケーション３０６（例えば、MS WORD、PowerPoint、又は、印刷）と関連付けられた保護文書を選択する。アプリケーション３０６は、実装可能ファイルシステム（ＩＦＳ）３１２にアクセスするため、ＡＰＩ（例えば、MS Windows（登録商標）において、Win32 APIによるcreateFile、Common Dialog File Open Dialog）を呼ぶ保護文書に作用する。「開く」要求がアプリケーション３０６からなされたことが検出された場合、この要求は、要求先の保護文書にアクセスするため、適当なファイルシステムドライバ（ＦＳＤ）３１４へ伝えられる。同時に、暗号モジュール３１０が作動され、認証されたユーザ鍵は、要求された保護文書のヘッダを復号化するためローカル記憶装置から取得される。暗号ヘッダが復号化さ

れ、その中のアクセス規則がユーザのアクセス特権との比較に合格したとき、ファイル鍵は保護文書のヘッダから取得され、暗号モジュール３１０は、ＤＳＭ３０２内で暗号文書を復号化する。クリアコンテンツは、ＩＦＳマネージャ３１２を介してアプリケーション３０６へ戻される。例えば、アプリケーション３０６がオーサリングツールである場合、クリアコンテンツは表示される。アプリケーション３０６が印刷ルールである場合、クリアコンテンツは指定されたプリンタへ送られる。

【００８０】「新」要求が検出された場合、すなわち、保護文書が作成若しくは執筆された場合、ファイル鍵がＤＳＭ３０２で（例えば、暗号モジュール３１０によって）生成され、このファイル鍵は、次に、作成中の文書のコンテンツを暗号化するため使用される。ローカル記憶装置が常に暗号文書を保持することを保証するため、処理若しくは作成されている文書内のどのようなコンテンツがＤＳＭ３０２のファイル鍵で暗号モジュール３１０を用いて暗号化されているとしても、毎回、「書き込み」要求（例えば、Microsoft Wordの「保存」コマンド）がユーザによって手動で行われ、或いは、アプリケーション３０６若しくはＯＳ３０４によって自動で行われる。「閉じる」要求がなされたとき、ファイル鍵は、ユーザが適用したあらゆるアクセス規則を含むヘッダに保持される。ヘッダは、次に、認証されたユーザ鍵で暗号化され、文書は、記憶装置３０８（例えば、フォルダ、若しくは、指定ロケーション）に記憶するため適当なＦＳＤ（例えば、３１４）へ送信される前に暗号文書に添付される。

【００８１】別の一実施例では、ProcessIDプロパティとして知られているオペレーティングシステム（ＯＳ）アクセスは、（AppActivateメソッドへの引数として）アプリケーションを作動するため使用される。パラメータProcessIDは、アプリケーションを識別し、そのアプリケーションのイベントハンドラは、種々のファイルシステムコンポーネントへのアクセスを調停する役割を担う実装可能ファイルシステム（ＩＦＳ）マネージャ３１２へのＯＳアクセスを継続するため、必要なパラメータを取る。特に、ＩＦＳマネージャ３１２は、ファイルを開く（オープン）、閉じる（クローズ）、読み取る（リード）、書き込む（ライト）などのプロセスのためのエントリーポイントとして機能するように構成される。一つ以上のフラグ若しくはパラメータを伝達することにより、このアクセスは、ＤＳＭ３０２を作動する。アプリケーションによってアクセス中の文書が通常（保護無し）である場合、文書は、一つのファイルシステムドライバ（ＦＳＤ）（例えば、ＦＳＤ３１４）から入手され、ＤＳＭ３０２を介して伝達され、次に、ＩＦＳマネージャ３１２を経由してアプリケーションにロードされる。これに対して、アプリケーションによってアクセスされる文書が保護されている場合、ＤＳＭ３０２は、暗号モジュール３１０を作動し、アクセス規則を取得するため、認証されたユーザ鍵の取得に進む。アクセス特権がアクセス規則を充たす場合、保護文書の暗号データ部を暗号器によって復号化するため、ファイル鍵が獲得される。その結果として、クリアモードのデータ部又は文書は、ＩＦＳマネージャ３１２を介してアプリケーションにロードされる。

【００８２】一実施例によれば、ＤＳＭ３０２は、動的リンクライブラリ（ＤＬＬ）のように構築されたファイル内のローカルディスク（例えば、図１Ｄの記憶装置１３６）に常駐し、典型的に、ＳＹＳ又はＩＦＳ拡張子をもち、システム初期化中にロードされる。ＤＳＭ３０２がインストールされ、初期化された後、カーネルは、ファイルオープン、リード、ライト、シーク、クローズなどの論理要求に関してＤＳＭ３０２と通信する。ＩＦＳマネージャ３１２を介して、ＦＳＤ３１４は、これらの要求を、それ自体のボリュームで見つけられる制御構造及びテーブルを用いて、セクタリード及びライトの要求に変換し、その要求のため、File System Helpers(FsHlps)と称される特殊なカーネルエントリーポイントを呼び出す。カーネルは、セクタＩ／Ｏの要求を適当なデバイスドライバへ渡し、その結果（例えば、要求された文書）をＦＳＤ３１４へ返す。ＦＳＤ３１４から、要求された文書が保護処理されている旨の結果を受信した後、ＤＳＭ３０２は、保護文書のアクセス規則によって許可されているならば、文書を復号化するため、内部の暗号モジュール３１０を作動する。

【００８３】図４Ａは、本発明の一実施例により作成された文書を保護する処理４００のフローチャートである。ステップ４０２で、ブランク文書がユーザによって選択若しくは作動されたオーサリングアプリケーションによって開かれるか、若しくは、作成される。好ましい一処理によれば、ユーザは、アクセス規則の組を用いて既に設立されたフォルダに文書を保存する。ステップ４０４で、所定のアクセス規則の組が受け取られ、好ましくは、マークアップ言語で受け取られる。上述の通り、アクセス規則は、望ましいアクセス規則、ユーザアクセス特権のデフォルト、或いは、個別に作成されたユーザアクセス特権を含む予め作成されたファイルのインポートによって取得してもよい。

【００８４】ステップ４０６で、秘密暗号鍵（すなわち、ファイル鍵）が文書用の暗号モジュールから生成され、典型的に、一般的に通常のユーザがアクセスできない一時ファイルに格納される。一時ファイルは、保護文書が（例えば、アプリケーションからの「閉じる」コマンドで）終了したときに、自動的に消去される。ステップ４０８で、文書をローカル記憶装置へ書き込む要求がなされたかどうかを調べるため文書が検査される。このような要求が検出された場合（この要求は、ユーザが手動で行う場合や、オーサリングツール若しくはＯＳが定

期的に行う場合がある）、文書は、ステップ４１０でファイル鍵を用いて暗号化される。本発明の特徴の一つは、保存された文書が、たとえ、処理中（例えば、作成中、編集中若しくは改訂中）であっても、常に記憶装置内で暗号化されている点である。ユーザが文書を終了したとき、「閉じる」要求は、文書を閉じるため有効にされる。ステップ４１２で、このような要求が検出される。このような要求が取得されると直ぐに、保護バージョンの文書が記憶装置に書き込まれる。ステップ４１３にいおいて、アクセス規則及びファイル鍵が、認証されたユーザ鍵で暗号化されたセキュリティ情報に収容される。実施形態に応じて、フラグ若しくは署名、及び、セキュリティ情報がヘッダに収容される。或いは、ヘッダは、フラグ無しのセキュリティ情報を収容してもよい。ステップ４１４で、ヘッダは、ステップ４１０からの暗号文書に添付され、次に、保護文書は、ステップ４１８で記憶装置に収容される。

【００８５】上述の通り、保護文書は、暗号セキュリティ情報を含むヘッダと、暗号データ部（すなわち、暗号文書）の二つの暗号部により構成される。この保護文書の二つの部分は、ファイル鍵とユーザ鍵の２個の異なる鍵で夫々に暗号化される。或いは、二つの暗号部は、ステップ４１６において、別の鍵で（若しくは、同じユーザ鍵を使用して）、再暗号化してもよい。

【００８６】特定のユーザ若しくはユーザのグループ毎に、多数のアクセス規則の組が存在する場合、ステップ４１３における暗号アクセス規則は、他の暗号アクセス規則の組と共に、図２Ｃ．２に示されるような規則ブロック内に一体化されることがわかる。このようにして、１ユーザ若しくは１グループからのアクセスは、他のユーザ若しくはグループに影響を与えないが、他のユーザ若しくはグループは、おそらく、更新バージョンの暗号文書を見ることができる。

【００８７】図４Ｂは、アクセス規則を取得する処理４３０の一例のフローチャートである。処理４３０は、図４Ａのステップ４０４で実行され、文書保護処理が容易に行えるようにする。ユーザに対する負荷を少なくするため、本発明は、後述のように、１回限りの認証機構を提供する。この認証機構は、ユーザ認証が保護文書へのアクセス毎に要求される従来技術のシステムとは著しく相違している。動作時に、一旦、ユーザが保護文書へのアクセスを認証されると、ユーザの認証は必要ではなくなる。また、ユーザの認証後は、ユーザは、再認証を受けることなく、他の保護文書へアクセスすることが可能である。

【００８８】一般的に、ユーザが保護文書にアクセスできるようになる前に認証されなければならない少なくとも二つの状況が考えられる。第１の状況では、クライアント装置はネットワーク（例えば、ＬＡＮ）に接続され、クライアント装置のユーザは、クライアント装置を最初に使用するときに、自分の資格情報を提供することによって自分を認証する必要がある。一般的に、資格情報は、ユーザ名とパスワードの組である。ユーザが登録済みであり、与えられた資格情報がサーバ内のユーザの識別情報と適合するならば、ユーザは認証される。ユーザが認証されると、ユーザに関連したユーザ鍵が有効にされるか、又は、認証される。ユーザは、クライアント装置を使用できるようになり、次に、保護文書にアクセスする。他の実現可能な資格情報は、例えば、クライアント装置に装備された専用装置から獲得できる指紋、音声などのようなユーザの生物測定情報を含む。このような装置の一例は、CA 94063, Redwood City, Suite 301, 805 Veterans Boulevard所在のDigitalPersonaインコーポレイテッドからの指紋センサである。ユーザの生物測定情報が捕捉されたとき、ユーザの主張する権利を検証することができる。実施形態に応じて、ユーザ鍵は、局部的に保存しても、遠隔的に取り出してもよい。何れの場合も、ユーザ鍵は、認証される前、ユーザ鍵に起こり得るハッキングを阻止するため、好ましくは、解読できないフォーマットである（例えば、ユーザと関連したパスフレーズで暗号化若しくはスクランブル処理されている。）。

【００８９】ユーザの認証、又は、ユーザの生物測定情報は、ユーザ鍵を有効とする、獲得する、或いは、認証するため使用される。その結果として、クリア形式で認証されたユーザ鍵は、ユーザが任意の保護文書にアクセスするため容易に利用できるようになる。第２の状況では、ネットワークに接続されたクライアント装置は、クライアント装置のユーザが保護文書の要求以外に実行する意向のある全てを許容することができる。保護文書への要求の場合、ユーザ認証処理が呼び出される。

【００９０】再度、図４Ｂを参照するに、ユーザ認証処理が呼び出され、サーバ（例えば、サーバ１０４若しくは１０６）への通信はステップ４３２で検査される。サーバへの利用可能な通信が検出されなかった場合、すなわち、クライアント装置がネットワーク上に存在しないか、サーバが停止しているか、或いは、他の原因がある場合、ユーザには、少なくとも３通りの選択の幅が与えられる。第１にユーザは、公開鍵が入手可能であるか、若しくは、クライアント装置に維持されている場合、ステップ４３４で、保護されていない文書だけにアクセスするか、又は、保護文書を生成することが可能である。第２に、ユーザは、サーバとの通信の試みを継続することができ、この場合、処理４３０は、保護通信リンクが確立されるまでステップ４３２へ戻る。第３に、ユーザは、本発明によって提供される別の特徴であるオフラインアクセスを巧く利用する。つまり、ユーザがクライアント装置上でアクセスする保護文書の数は制限されている。詳細については後述する。

【００９１】安全なリンク（できれば、ＨＴＴＰＳ、Ｖ

ＰＮ、ＳＳＬを経由する）がクライアント装置とサーバの間に確立された場合を考える。処理４３０は、ステップ４３６へ進み、ユーザ及び／又はクライアント装置自体を認証する必要がある。一部のケースでは、保護文書は、許可された装置からのユーザだけによってアクセスされることが保証される必要がある。したがって、このようなケースでは、ユーザと、ユーザが保護文書にアクセスすえる時のクライアント装置と、を認証する必要がある。

【００９２】ユーザに関する限り、ユーザは、検証されるべき自分の資格情報（例えば、ユーザ名／パスワード）を提供する必要がある。ユーザがサーバによって認証された後、クライアント装置を認証する必要がある。ユーザが１台以上の指定されたローカル・コンピュータに制限され、ユーザがこれらの指定されたローカル・コンピュータからの保護文書だけにアクセスすることを保証するため、ユーザが保護文書にアクセスする指定されたローカル・コンピュータのうちの１台を使用するかどうかを決定する。動作中に、ステップ４３６で、

１）このクライアント装置が保護文書にアクセスするため使用できるかどうか並びに、

２）クライアント装置とユーザの組み合わせが有効であるかどうかを決定するため、クライアント装置の識別子（例えば、ネットワークカードからの番号）がサーバによって検査される。この検査処理が成功したとき、処理４３０はステップ４３８へ進み、さもなければ、ユーザは、ステップ４３４で保護されていない文書だけに対して作業を行う。

【００９３】ユーザに関連したユーザ鍵はステップ４３８で認証される。この時点で、ユ＾ザは、保護文書にアクセス可能である。確実に、ユーザの対応したアクセス特権と、保護文書のアクセス規則は、ユーザが保護文書を開くことができるかどうかを、最終的に決定する。

【００９４】ユーザと、このユーザが使用するクライアント装置が、それぞれ、認証若しくは検証された後、ユーザ鍵が有効な状態になる（例えば、使用する準備が整う。）。ユーザ鍵は、解読できないフォーマットで新たに生成されるか、若しくは、保存される。ユーザ認証処理は、容易に使用できる形式でユーザ鍵を取得するか、及び／又は、ユーザ鍵をクライアント装置に与える。

【００９５】ユーザが保護文書にアクセス中、若しくは、保護文書を編集中である場合を想定する。ステップ４４０で、管理者によって最初に設定されたユーザアクセス特権が有効状態にされ、このユーザアクセス特権は、ユーザが保護文書にアクセスすることができるとき、場所、及び、種類を決定する。同様に、保護文書を格納する特定のフォルダに対するデフォルトアクセス規則は、ステップ４４２において、閲覧のため利用可能にされ、或いは、収集される。このデフォルトアクセス規則は、ユーザによってアクセスされるか、作成される暗号文書へ最終的に（暗号フォーマットで）添付される一時ファイルに保存することができる。

【００９６】図４Ｂにおける処理４３０の説明は、サーバと連動して形成されたユーザ認証処理に基づいている。しかし、当業者に明らかであるように、この説明はユーザ認証を実行するための他の手段に容易に適用される。例えば、ユーザ鍵は、上述の通り、ユーザの生物測定情報によって認証、検証、或いは、取得される。

【００９７】図４Ｃを参照するに、一実施例による保護文書アクセス処理４５０のフローチャートが示されている。これは、図３と併せて理解されるべきである。ステップ４５２において、アプリケーションは、指定された文書と共に始動される。例えば、WINWORD.EXEがファイル名xyz.docのファイルを開くため作動される。上述の通り、ＯＳからのハンドラは、アプリケーションを識別し、ＯＳに入り、ステップ４５４でＩＦＳマネージャが呼び出される。ＩＦＳマネージャはステップ４５６でＤＳＭモジュールを作動し、同時に、ＩＦＳマネージャは、ステップ４５８で、選択された文書を記憶装置から取得するためハンドラをパスする。選択された文書はＤＳＭモジュールを通過するので、選択された文書は、ステップ４６０で、保護されているか、保護されていないかが判定される。一般的に、選択された文書の保護特性を検査するため少なくとも２通りの方法がある。考えられる第１の方法は、ＤＳＭモジュールが文書の先頭のフラグを捜すことである。上述の通り、一部の保護文書では、所定のデータの組のようなフラグが、アクセス対象の文書が保護されていることを示すためにヘッダに配置されている。このようなフラグが見つからない場合、処理４５０はステップ４７０へ進む。すなわち、選択された文書は、保護されていないと考えられ、ＤＳＭモジュールを通過することが許可され、ＩＦＳマネージャからアプリケーションへロードされる。考えられる第２の方法は、ＤＳＭモジュールが保護文書のヘッダを探すことである。保護文書の場合、ヘッダが暗号データ部に添付される。ヘッダのデータフォーマットは、保護されていない文書と比較すると、不規則であるべきである。ＤＳＭモジュールが、アプリケーションによって要求されるような不規則なデータフォーマットは選択された文書に存在しない、と判定した場合、この処理４５０はステップ４７０へ進む。すなわち、選択された文書は、保護されていないと考えられ、ＤＳＭモジュールを通過することが許可され、ＩＦＳマネージャからアプリケーションへロードされる。

【００９８】ステップ４６０において、選択された文書が本当に保護されていると判定された場合、処理４５０はステップ４６２へ進み、ヘッダ又はヘッダ内のセキュリティ情報は認証されたユーザ鍵で復号化される。ステップ４６４で、復号セキュリティ情報内のアクセス規則が取得あれる。ステップ４６６で、アクセス規則は、ユ

ーザに関連したアクセス特権と比較される（照合される。）。照合に失敗した場合、すなわち、ユーザが特定の文書にアクセスすることを許可されていない場合、通知若しくは警告メッセージがＤＳＭモジュールによって生成され、ステップ４６７でユーザに提示される。或いは、アプリケーション自体が選択された文書のオープンに失敗したときに警告メッセージを表示してもよい。この照合に合格した場合、すなわち、ユーザが特定の文書へのアクセスを許可されたとき、ファイル鍵は、ステップ４６８でセキュリティ情報から取得され、選択された（保護）文書の暗号データ部を、ＤＳＭモジュールによって作動された暗号モジュールで復号化するため使用される。その結果として、ステップ４７０において、復号文書又は選択された文書のクリアコンテンツがＩＦＳマネージャからアプリケーションへロードされる。

【００９９】図５Ａを参照するに、１台以上のプロセッサ５０１によって実行可能であるサーバ・モジュール５０２がメモリ空間５０３に搭載されたサーバ装置５００の機能ブロック図が示されている。サーバ装置５００は、ネットワーク上のサーバ５００及び他の装置と、ローカル記憶空間５０５との間での通信を容易に行わせるためのネットワーク・インタフェース５０４を含む。サーバ・モジュール５０２は、本発明の一実施例の実行可能なバージョンであり、実行されたとき、本発明で熟考された特徴／結果を生じる。一実施例によれば、サーバ・モジュール５０２は、管理インタフェース５０６と、アカウント・マネージャ５０８と、ユーザ鍵マネージャ５１０と、ユーザ・モニタ５１２と、ローカル・サーバ・マネージャ５１４と、パートナー・アクセス・マネージャ５１６と、アクセス報告マネージャ５１８と、規則マネージャ５２０とを具備する。

【０１００】管理インタフェース５０６について

名前から分かるように、管理インタフェース５０６は、システム管理者がユーザを登録し、夫々のアクセス特権をユーザに許可することを容易に行わせ、全てのサブモジュール、又は、その結果が初期化され、更新され、管理されるサーバ・モジュールへのエントリーポイントである。一実施例において、システム管理者は、種々のアクティブフォルダー、記憶ロケーション、ユーザ若しくはユーザのグループのための階層アクセスレベルを設定する。例えば、図５Ｂ．１に示されるように、異なるユーザには、異なるアクセス特権が割当てられる。ユーザＡは、任意の保護文書へのアクセス特権が与えられた幹部若しくは支店長である。ユーザＢはアクセス特権が制限され、ユーザグループＣの全てのメンバは同じアクセス特権を共用する。特権には、開く、編集する、書き込む、印刷する、コピーする、ダウンロードする、或いは、その他の特権が含まれるが、これらの例に限定されるものではない。他の特権の例には、他のユーザのアクセス特権の変更、一つ以上のロケーションからの保護文書へのアクセス、前に設定されたものとは異なるフォルダ用のアクセス規則の組の設定などが含まれる（これらは、おそらくシステム管理者が行う。）。ユーザに割り当てられたそれぞれのユーザＩＤを用いることによって、全ユーザのマネージメントが容易になる。特に断らない限り、ユーザ若しくは対応したユーザＩＤは、人であるユーザ、ソフトウェアエージェント、ユーザのグループ、及び／又は、ソフトウェアエージェントのグループを識別するため互換的に使用される。保護文書にアクセスすることを要求するユーザだけではなく、ソフトウェアアプリケーション又はエージェントは、フォワードを進めるため保護文書にアクセスする必要の生じる場合がある。従って、特に断らない限り、「ユーザ」という用語は、必ずしも人を意味するとは限らない。一般的に、保護文書にアクセスするユーザには、保護文書中の暗号ヘッドを解読（復号化）させることができるユーザ鍵が関連付けられる。ユーザ鍵の期限切れ、若しくは、再発行は、システム管理者によって始められる。一実施例によれば、管理インタフェース５０６は、認証されたシステム管理者又は運営者が実行すべき様々なタスクに対する選択範囲を提示するユーザ・グラフィック・インタフェースである。

【０１０１】アカウント・マネージャ５０８について

原則的に、アカウント・マネージャは、全登録ユーザと、各登録ユーザのアクセス特権と、そして、おそらく対応したユーザ鍵（例えば、秘密鍵及び公開鍵）とを保持するデータベース、若しくは、データベース５０７（例えば、オラクルデータベース）へのインタフェースである。動作時に、アカウント・マネージャ５０８は、ユーザがサーバ５００にログオンしたときにユーザを認証し、ユーザが現在の場所（ロケーション）から保護文書にアクセス可能であるかどうかを判定する。一般的に、アカウント・マネージャ５０８では、企業がその企業のユーザを制御することができる。

【０１０２】ユーザ鍵マネージャ５１０について

このモジュールは、組織のユーザ毎に鍵のコピーを持ち続けるように構成される。一実施例によれば、ユーザ鍵マネージャ５１０は、鍵を獲得するために作動されるものではない。ある状況では、鍵は、クライアント装置内の鍵が改竄されるか、若しくは、保護文書にアクセスするアクセス特権を与えられたユーザがこれ以上通用しなくなるケースにおいて、保護文書にアクセスするためシステム管理者によって獲得される。オプションとして、ユーザ鍵マネージャ５１０は、セキュリティ上の理由から一部若しくは全部の鍵を失効させるように構成される。ある種のケースでは、ユーザは組織から離れ、対応したユーザ鍵はユーザ鍵マネージャ５１０内で手入力で失効させられる。別のケースでは、ユーザの鍵は、長期に亘って使用され、ユーザ鍵マネージャは、旧いユーザの鍵を失効させ、旧いユーザの鍵を新たに生成された鍵

で置換する。このような置換は、ユーザに気付かれないようにして行われ、新しい鍵は、ユーザが次にログオンしたときからクライアント装置にアップロードされる。別の実施例によれば、ユーザ鍵マネージャ５１０は、ユーザ毎に秘密鍵と公開鍵を持ち続ける。公開鍵は、ヘッダのセキュリティ情報を暗号化するため使用され、秘密鍵はヘッダのセキュリティ情報を復号化するため使用される。図５Ｂ．２は、アカウント・マネージャ５０８と協働してユーザ鍵マネージャ５１０によって保持し続けられた表の一例の説明図である。

【０１０３】ユーザ・モニタ５１２について

このモジュールは、ユーザの要求及び居所を監視するため構成される。典型的に、ユーザは、１箇所以上の指定ロケーション、若しくは、ネットワーク接続されたコンピュータから保護文書にアクセスすることが許可される。ユーザがより高いアクセス特権を与えられている場合（例えば、ロケーション若しくはネットワーク接続されたコンピュータ以外からのアクセスが許可されている場合）、ユーザ・モニタ５１２は、ユーザが常に登録済みロケーション又はコンピュータのうちの一つから一つのアクセス権限だけを与えられることを保証するように構成される。その上、ユーザ・モニタ５１２は、アクセス特権の更新を定期的に押し進めるか、又は、アクセス特権の更新の要求に応答するように構成され、スケジューリングされる。

【０１０４】ローカル・サーバ・マネージャ５１４について

このモジュールは、所定のロケーション、又は、所定のユーザのグループのために機能するローカル・サーバのため適切なローカル・モジュールを配布する役目を果たすように設計される。一実施例によれば、ローカル・サーバ・マネージャ５１４は、サーバ５００で実行されるサーバ・モジュール５１４の一部又は全部を複製し、複製されたコピーを全てのローカル・サーバに配布する。その結果として、ユーザは、単一の中央サーバ、すなわち、サーバ５００の認証を受けることなく、ローカル・サーバが対象とするネットワーク施設内のどこからでも、保護文書にアクセスすることができる。別の実施例によれば、ローカル・サーバ・マネージャ５１４は、サーバ５００で実行されるサーバ・モジュール５０２の一部を複製し、対応したローカル・サーバへ配布する。この実施例の場合、各ローカル・サーバは、サーバ・モジュール５０２から個別に作製された複製を具備する。ユーザに十分に高いアクセス特権が与えられている（例えば、２箇所以上のロケーション若しくは２台以上のコンピュータからのアクセスが許可される）とき、ユーザ・モニタ５１２は、ユーザがあるローカル・サーバによるサービスを受ける最初に構成されたロケーションから、別のローカル・サーバによるサービスを享受する別の許可されたロケーションへ移動したことを検出することができる。通知の後、ローカル・サーバ・マネージャ５１４は、ユーザが新たに連絡を取ったローカル・サーバのためのローカル・モジュールを再構成するように設定される。すなわち、ユーザは、新たに連絡を取ったローカル・サーバにユーザとして追加される。ユーザが組織内の何処に居るかとは無関係に、同時には１台のコンピュータからしかアクセスできないことが要求される場合、ローカル・サーバ・マネージャ５１４は、ユーザが前に連絡を取っていたローカル・サーバのためのローカル・モジュールを再構成することが可能である。その結果として、ユーザは、そのユーザが前に連絡を取っていたローカル・サーバから削除される。

【０１０５】パートナー・アクセス・マネージャ５１６について

これは、非従業員のアカウントを管理するための特殊モジュールである。非従業員は、コンサルタントがある種の保護文書にアクセスすることを要求するビジネスに対するコンサルタントでもよい。パートナー・アクセス・マネージャ５１６は、一般的に、サーバのモジュールに従って動作するが、パートナー・アクセス・マネージャ５１６によって直接管理されているようなユーザに付加的な制約を加える。あるアプリケーションでは、パートナー・アクセス・マネージャ５１６は、コンサルタントとの契約が終了したとき、コンサルタントのための鍵又は鍵ペアを失効させるため、ユーザ鍵マネージャ５１０への要求を生成する。

【０１０６】アクセス報告マネージャ５１８について

このモジュールは、起こり得るアクセス行動を記録若しくは追跡するように設定され、主として、クライアント装置で実行されるクライアント・モジュール内の対応したサブモジュールと共に機能する。アクセス報告マネージャ５１８は、好ましくは、システム管理者によって作動され、アクセス報告マネージャ５１８に集められたコンテンツは、システム管理者又は権限のある人だけによってアクセスされる。

【０１０７】規則マネージャ５２０について

一般的に、規則マネージャ５２０は、様々なアクセス規則の執行機構である。一局面によれば、規則マネージャ５２０は、i)データタイプ（例えば、Microsoft Word（登録商標））、ii)グループユーザ又は個人、iii)適用権利、及び、iv)アクセス規則の期間に基づいて規則を指定するよう構成される。典型的に規則の組はポリシーである。ポリシーは、許可状態にすること、禁止状態にすること、編集すること、配備すること、及び、取り消すことが可能である（例えば、１乃至２レベル）。規則マネージャ５２０によって管理されるポリシーは、好ましくは、大域的レベルで動作する。ポリシーは、ログインプロセス中に（ユーザが認証された後に）クライアント装置にダウンロードされ、動的に更新される。更に、それぞれのポリシーは、アクティブ状態のフォルダ

（すなわち、保護文書を保存するため指定された場所）と関連付けられる。これらのポリシーは、クライアント装置にダウンロードされ、更新される。簡単なポリシーは、文書に埋め込まれ、文書専用ポリシーを与える。一実施例によれば、ヘッダは、ローカル・サーバによってクライアントから取得され、ヘッダからアクセス規則が取り出される。鍵マネージャ５１０は、ヘッダの暗号セキュリティ情報を復号化するため呼び出される。規則マネージャ５２０は、セキュリティ情報からのアクセス規則を解析し、保護文書がユーザによってアクセス可能であるかどうかを判定すべくアクセス規則をユーザのアクセス特権と評価又は比較するため呼び出される。評価又は比較が成功したとき、ファイル鍵は取り出され、クライアントへ返送される。

【０１０８】尚、図５Ａのサーバ・モジュール５０２は、本発明の一実施例による一部の例示的なモジュールを列挙しているが、本発明を実施するためには、必ずしもサーバ・モジュール５０２の全てのモジュールを組み込まなくてもよい。記載された事項から当業者には明らかであるように、モジュールとモジュールの変形の様々な組み合わせは、本発明の精神を逸脱することなく、本発明において熟考された種々の望ましい機能、利益及び効果を達成する。

【０１０９】図５Ｂ．３を参照するに、ユーザ鍵を更新する処理５１０のフローチャートが示されている。上述の如く、ある種のケースでは、ユーザ鍵の期限を終了させること、及び、失効したユーザ鍵を新しいユーザ鍵で更新することが必要である。好ましくは、処理５１０は、例えば、ユーザがサーバにログオンするときに、ユーザに気付かれることなく進められる。オプションとして、ユーザは、自分のユーザ鍵の更新が通知される。一般的に、ユーザ鍵の失効／更新を要求する少なくとも２通りの状況がある。ユーザが組織を離れるとき、セキュリティ上の理由から、そのユーザに関連したユーザ鍵を無効にすることが望ましい。したがって、ステップ５１１では、処理５１０は手動による要求を待ち受ける。システム管理者に従業員の離職が通知されたとき、このような手動による要求が行われ得る。

【０１１０】或いは、組織又はシステム管理者は、失効したユーザ鍵を新しいユーザ鍵で置換するため、例えば、６ヶ月単位で、マネージメント下のあらゆるユーザ鍵の期限切れのタイムテーブルを設定することができる。ステップ５１２において、この処理は時限要求を待ち受ける。

【０１１１】何れのケースでも、処理５１０がステップ５１１若しくはステップ５１２からの要求で進行させられるとき、ステップ５１４において、サーバ・モジュールの鍵マネージャは、対象にされているユーザ鍵又は探し求められているユーザ鍵を調べるため参考にされる。対象の鍵が取得されたとき、対応した新しい鍵が暗号技術によってステップ５１６で生成される。一実施例によれば、使用される暗号は、保護文書のヘッダを暗号化／復号化するためクライアント・モジュールで使用された暗号と同一であるか、又は、実質的に同一である。これにより、新たに生成されたユーザ鍵が、クライアント装置で利用可能であるときに使用できることが保証される。別の実施例によれば、ユーザに関連した鍵のペアが更新される。２個の鍵は、サーバに保持され、決してサーバから外に出されないので、適当な暗号がユーザ鍵を更新する用途に適用可能である。

【０１１２】ユーザ鍵が置換される実際の状況及び実施形態に応じて、新たに生成された鍵は、鍵マネージャに留め置かれるか、又は、次に対応したユーザがクライアント装置からログオンしたときにクライアント装置へ引き渡される。ステップ５１８において、処理５１０は、新たに生成された鍵をサーバ側に残すか、又は、クライアント側にダウンロードされるかの決定を待つ。新たに生成された鍵をサーバに維持することが決定された場合、処理５１０はステップ５２０へ進み、新しい鍵は、同じユーザと関連付けられる。次にユーザがサーバにログオンしたときに、新たに生成された鍵をユーザへ引き渡すことに決定された場合、処理５１０はステップ５２２へ進む。ステップ５２２において、処理５１０はユーザからの連絡（接触）を待つ。上述のように、ユーザは、保護文書へアクセスする必要があるとき、クライアント装置からいつでもログオンできる。このような連絡が生じたとき、サーバは、自分が資格保持者であることを裏付けようとするユーザから資格情報を受け取る。ユーザが認証された後、新しい鍵は、ステップ５２４で資格情報を用いて暗号化される。資格情報は、認証を要求するときユーザによって与えられ、ユーザ名とパスワードの組、又は、ユーザの生物測定的特徴（例えば、指紋）を含む。どのような暗号が使用されるかとは無関係に、新たに生成された鍵は、ステップ５２６において、クライアント装置へアップロードされるか、又は、伝送される。暗号化された新しい鍵を受信した後、クライアント装置は、ステップ５２８において、新しいユーザ鍵が保護文書にアクセスするため、又は、文書を保護するため容易に利用できるようにするため、暗号化された新しい鍵を復号化する状態になる。一部のケースでは、クライアント装置のクライアント・モジュールは、指定されたフォルダ内で、旧いユーザ鍵で原始的に暗号化されたヘッダを有する利用可能な全保護文書を調べる（スキャンする）ようにスケジューリングされる。これらの文書は、保護文書が本当に保護されていることを保証するため、新しい鍵を用いて再度暗号化される。好ましい一実施例によれば、ユーザ鍵の更新は、ユーザに関する限り、気付かれないように実行することができる。換言すると、ユーザは、処理５１０が行われていること、並びに、新しい鍵がインストールされたことに気が付かな

い。

【０１１３】図５Ｂ．４を参照するに、本発明の一実施例に従って保護文書にアクセスするサーバ支援処理５３０のフローチャートが示されている。処理５３０については、図４を参照して説明する。処理５３０の特徴のうちの一つは、後述されるように、ユーザ鍵（すなわち、秘密鍵及び公開鍵）が、鍵を生成したサーバから外に出ないことであり、これにより、鍵のセキュリティのレベルが向上する。

【０１１４】ユーザがクライアント装置から保護文書にアクセスしようとし、アクセス制御マネージメントを動かすサーバ（例えば、サーバ５００）によって認証された場合を想定する。保護文書が選択されたとき、図３の文書保護用モジュール（ＤＳＭ）３０２は、保護文書内のセキュリティ情報にアクセスするためユーザ鍵が要求されることを判定する。本実施例によれば、ＤＳＭ３０２は、保護文書からヘッダを分離し、そのヘッダをサーバへ送信するように構成される。ステップ５３２において、このようなヘッダがクライアント装置から受信される。後述のように、ヘッダは、暗号形式のセキュリティ情報を含む。ステップ５３４において、ユーザと関連した秘密ユーザ鍵が取り出される。秘密ユーザ鍵は、例えば、鍵マネージャから取り出される。ヘッダ内の暗号セキュリティ情報は、次に、ステップ５３６において、取り出された秘密ユーザ鍵で復号化される。その結果として、この保護文書用のアクセス規則はステップ５３８で獲得される。

【０１１５】同時に、ユーザのアクセス特権がステップ５４０で取り出される。アクセス特権は、例えば、アカウント・マネージャから取り出される。アクセス特権と文書のアクセス規則が与えられた場合、アクセス権が許可され得るかどうかを決定するため、ステップ５４２において、評価が行われる。ユーザのアクセス特権がアクセス規則に応じたアクセスを許可しない場合、処理はステップ５４４へ進む。ステップ５４４において、クライアント装置へ転送するためのエラーメッセージが生成され、これにより、ユーザは、自分のアクセス特権が選択された文書にアクセスすることを許容しないことを知る。しかし、他方で、ユーザのアクセス特権がアクセス規則に従ったアクセスを許可する場合、処理はステップ５４６へ進む。ステップ５４６において、セキュリティ情報内のファイル鍵が取り出される。ステップ５４８において、ファイル鍵はクライアント装置へ転送される。ファイル鍵を受け取った場合、ＤＳＭ３０２は、選択された文書の暗号データ部を復号化するため暗号モジュール３１０を作動する。

【０１１６】図５Ｂ．５は、本発明の一実施例による文書保護のサーバ支援処理５５０のフローチャートである。処理５５０について、図３を参照して説明する。ユーザは文書を仕上げた直後であり、文書を保護することを決定した場合を考える。文書を保護するために考えられる一つの方法は、上述のように、プリセットされた指定フォルダ、又は、アクセス規則の組と関連付けられた指定フォルダにその文書を収容することである。換言すると、フォルダ内の全文書は、実質的に同じアクセス規則が与えられる。

【０１１７】したがって、ＤＳＭ３０２が作動され、ＤＳＭ３０２は、次に、暗号モジュール３１０を作動する。文書が始めて保護処理される場合、暗号モジュール３１０は新しいファイル鍵を生成する。ファイル鍵が既に存在する場合、典型的に、暗号モジュール３１０は、要求されない限り、新しいファイル鍵を生成しない。処理５５０が開始する前に、ユーザは認証され、クライアント装置とサーバの間のリンクは確立されている場合を想定する。

【０１１８】クライアント装置からステップ５５２でファイル鍵を受信した後、ユーザに関連した公開ユーザ鍵が、ステップ５５４で、例えば、鍵マネージャから取り出される。文書用のアクセス規則は、ステップ５５６で取得される。上述の如く、アクセス規則は多数の方法で取得することができる。考えられる一つの方法は、クライアント装置から直接的にアクセス規則を受け取ることである。考えられる別の方法は、文書がシステムによって設定されたフォルダに格納されている場合に、局所的に規則マネージャからアクセス規則を取得することである。アクセス規則及びファイル鍵が与えられた場合、ステップ５５８でセキュリティ情報を形成することが可能になる。セキュリティ情報は、ステップ５６０で、公開ユーザ鍵を用いて暗号化される。図２Ｃ．２に類似した一実施例によれば、アクセス規則及びファイル鍵は、規則ブロック内に既に他のセグメントが存在する場合、セグメントに配置される。

【０１１９】ステップ５６２において、文書用のヘッダが生成される。実施形態に応じて、ヘッダは、暗号化されないその他の情報（例えば、フラグ）を含み得る。或いは、現在ユーザを含むユーザブロックがヘッダに追加される。ヘッダは、ステップ５６５でクライアント装置へ転送され、クライアント装置では、ヘッダは、保護文書を生成するため、暗号データ部に添付されるか、又は、暗号データ部と一体化される。尚、処理５５０は、保護文書が改訂され、記憶装置に保存されるときにも適用可能である。

【０１２０】図５Ｃは、ローカル・サーバ装置５７０の機能ブロック図である。ローカル・サーバ装置５７０は、一般的に、図５Ａに示されたサーバと類似している。従って、図５Ｃに示された多数の部品については、本発明の局面が分かり難くなることを避けるため、繰返して説明しない。図５Ｃに示されるように、ローカル・サーバ装置５７０は、図５Ａのサーバ・モジュール５０２の完全な複製又は部分的な複製となるように設定され

たローカル・モジュール５７０と称されるモジュールを実行する。本発明の特徴の一つとして、ローカル・モジュール５７２は、図５Ａの中央サーバ５００によって遂行される集中アクセス制御マネージメントの信頼性、確実性、及び、拡張性を提供する。このため、アクセス制御マネージメントの制御を失うことなく、必ずしも全ての認証要求を１ヶ所の中央ポイントで取り扱う必要がなくなる。本発明の別の特徴として、ユーザは、中央サーバがメンテナンスのため停止された場合、並びに、中央サーバへのコネクションが利用できない場合、影響されない。多数のローカル・サーバが使用され、各ローカル・サーバがサーバ・モジュールの複製を有するとき、ユーザに提供するサービスの信頼性は、著しく改善される。ユーザが保護文書へアクセスすることを希望し、認証され得ない可能性は、最小限に抑えられる。

【０１２１】一実施例によれば、ローカル・モジュール５７２は、中央サーバ５００におけるサーバ・モジュール５０２のある種の局在化されたバージョンであり、ローカル・サーバの近くのユーザへサービスを提供する。例えば、図５Ｄには、中央サーバ５００によって管理される全ユーザの表５８４が示されている。ユーザの中で、Ｊｏｈｎのアクセス特権５８５は、レベル１０（最高レベルと考えられる）であり、３箇所のあらゆるロケーションから、いつでも、毎日、保護文書にアクセスすることが可能である。Ｄｅｌｌのアクセス特権５８６はレベル１（最低レベルである）であり、ロケーションＡだけから、月曜から金曜まで、一日につき８時間（例えば、午前９時から午後５時まで）、保護文書にアクセスすることが可能である。Ｍｉｋｅのアクセス特権５８６は、レベル５であり、月曜から土曜まで１日１２時間、ロケーションＡ及びＢから、保護文書にアクセスすることができる。ローカル・サーバが３箇所のロケーションＡ、Ｂ及びＣに対して別々に利用される場合、図５Ｅに示されるように、ローカル・サーバ毎に割当てられた３種類のアクセス制御マネージメントの可能性が存在する。その結果として、ローカル・ユーザは、対応したローカル・サーバだけで検査をすればよく、ユーザは、他のローカル・サーバがいかなる理由で停止している場合であっても、或いは、中央サーバから切り離されている場合であっても、影響を受けることがない。

【０１２２】図５Ｆには、ユーザ毎のアクセス可能性が示されている。サーバ・モジュール５００のユーザ・モニタ５１２と共に動作することにより、ローカル・モジュール５７２は、動的に構成することが可能になる。一実施例では、３個のローカル・モジュールを設けて、夫々のローカル・モジュールでＪｏｈｎが３箇所の何れのロケーションからでもアクセスできるようにする代わりに、Ｊｏｈｎが同時にアクセスすることができるロケーションは、３箇所のロケーションのうちの一つのロケーションとなるように１個のローカル・モジュールだけが設定される。この動的コンフィギュレーション機構によって実現される付加的なセキュリティの効果の一つは、Ｊｏｈｎが保護文書にアクセスできるロケーションは、同時には、一箇所のロケーションに限られることである。実際には、これは、同時に二箇所の物理的な場所からシステムにログインし、又は、保護文書にアクセスする人にとっては望ましくないセキュリティ機能である。また、セキュリティ上の理由から、好ましくは、ユーザは、自分のアクセス特権とは無関係に、同時には一箇所のアクセスロケーションしか許可されない。

【０１２３】図５Ｇには、アクセス制御マネージメントに影響を与える動的コンフィギュレーションが示されている。ある時に、システムは、Ｊｏｈｎがロケーション Ａからアクセスしていることを認識する。Ｊｏｈｎがロケーション Ｂへ移動したとき、Ｊｏｈｎのログイン時に、中央サーバ（例えば、サーバ・モジュールのユーザ・モニタ）は、Ｊｏｈｎの居所を検出し、ローカル・サーバ・マネージャ５１４に対して、ロケーションＡとロケーションＢの両方のローカル・モジュールを再構成するように通知する。図５Ｇに示されるように、ロケーションＡのローカル・サーバにおけるローカル・アクセス制御マネージメント５８９は、Ｊｏｈｎに対する役割が終わり、ロケーションＢのローカル・サーバ内のローカル・アクセス制御マネージメント５９０がＪｏｈｎのための機能を引き継ぐ。その結果として、Ｊｏｈｎは、ロケーションＢから保護文書にアクセスすることが許可されるが、ロケーションＡからはアクセスできなくなる。図５Ｈは、Ｊｏｈｎのアクセス可能性がロケーションＡからロケーションＢへ移動したことをグラフィック表現した図である。このように、Ｊｏｈｎは、Ｍｉｋｅと共に、ロケーションＢから保護文書へアクセスすることが可能であり、両者は、一時的に、ロケーションＡから保護文書へアクセスすることを許されなくなる。

【０１２４】Ｍｉｋｅがロケーション Ａを移動した場合、ローカル・モジュールは、図５Ｉに示されるように再構成される。Ｊｏｈｎのアクセス特権のため、Ｊｏｈｎは、ロケーションＣへ移動した場合、ロケーションＣから保護文書へアクセスすることが可能になる。

【０１２５】図６Ａは、中央サーバ５００又はローカル・サーバ５７０に組み込まれるユーザ認証処理６００のフローチャートである。上述のように、ネットワーク接続されたクライアント装置への初期ログインと、保護文書への最初のアクセスの少なくとも２通りの状況で処理６００が要求される。いずれかの状況が出現したとき、クライアント装置内のクライアント・モジュールは、処理６００をスタートさせるため、アクセス制御マネージメントを行うモジュールを動かすサーバに送られた要求を開始する。

【０１２６】ステップ６０２において、サーバは要求を待ち受ける。クライアント装置から要求を受信すると、

サーバは、ステップ６０４へ進み、ユーザと、ユーザが保護文書にアクセスするため使用するクライアント装置とが、認証済みであるか銅かを判定する。両方が既に認証されている場合、ユーザ若しくはクライアント装置に対してこれ以上の認証処理がなされることはない。これに対して、ユーザとクライアント装置が未だ認証されていないとき、認証処理が続けられる。一実施例によれば、サーバは、サーバとクライアント装置の両方が公開ネットワークに接続されている場合には、クライアント装置との間で安全なリンクを確立する。このようなリンクは、ＨＴＴＰＳを利用するか、又は、ＶＰＮを通じてサポートされる。或いは、別の認証手段が利用されている場合には、クライアント装置とサーバの間に直接リンクが確立される。

【０１２７】ステップ６０６において、サーバは、認証応答と共に受信された要求に応答する。実施形態に応じて、このような応答は、クライアント装置のスクリーンに表示されるべきダイアログ・ボックス、コマンド、或いは、その他の要求である。何れのケースでも、この応答は、資格情報がユーザによって与えられることを要求する。上述の如く、資格情報は、ユーザ名とパスワードの組、又は、ユーザの生物測定情報などであり、認証処理が先へ進む前に、ステップ６０８でユーザから受け取る必要がある。

【０１２８】ステップ６１０において、資格情報を受信したとき、サーバは、ユーザがリポジトリ、ローカル記憶装置、サーバ自体、又は、ネットワーク経由でアクセス可能なその他の装置に保持された保護文書にアクセスすることを許可されたユーザであるかどうかを判定する必要がある。この判定には、受け取った資格と、サーバに予め記憶されているものとの照合が含まれる。尚、サーバは、中央サーバでもローカル・サーバでも構わない。当業者に明らかであるように、この解説は、どちらの状況でも同じように当てはまる。照合に失敗した場合、すなわち、ユーザが認証されていない場合、処理６００は先頭へ戻り、要求の待ち受けを続ける。換言すると、保護文書へのアクセス、又は、システムへのログインのための現在の要求は放棄される。商号に成功した場合、ユーザは認証されたユーザであると認められる。

【０１２９】同時に、クライアント装置は、おそらく、そのＩＰアドレス、又は、ネットワーク・カード識別情報、又は、クライアント装置を個別に識別するその他の手段によって類似した認証を受ける。

【０１３０】ユーザとクライアント装置の両方が認証された場合、処理６００はステップ６１２へ進み、ユーザのアクセス特権が取り出され、有効な状態にされる。実施形態に応じて、ユーザのアクセス特権を有効にすることは、アクセス特権を含むファイルをクライアント装置へダウンロードすること、アクセス特権を含むローカル・ファイルを復号化すること、又は、単にサーバのメモリ空間内でユーザを有効な状態にすることである。何れのケースでも、このポイントで、ユーザのアクセス特権は、容易にアクセス可能であり、ユーザは認証されたクライアント装置から保護文書にアクセスすることが許可される。

【０１３１】一実施例によれば、ＸＭＬ－ＲＰＣが、サーバ（例えば、ローカル・サーバ若しくは中央サーバ）とクライアント装置との間の通信を容易に実現するため使用される。ＸＭＬ－ＲＰＣは、ＨＴＴＰを用いてリモート・プロシージャ・コールを行うための簡単且つポータブルな方法である。ＸＭＬ－ＲＰＣは、Ｐｅｒｌ、Ｊａｖｅ、Ｐｙｔｈｏｎ、Ｃ、Ｃ＋＋、ＰＨＰ、及び、その他のプログラミング言語と共に使用することが可能である。更に、ＸＭＬ－ＲＰＣは、異なるオペレーティングシステムで動くソフトウェア、異なる環境で動くソフトウェアに、データネットワークを介するプロシージャ・コールを行わせることが可能である。これは、トランスポートとしてＨＴＴＰを使用し、エンコーディングとしてＸＭＬを使用するリモート・プロシージャ・コールである。ＸＭＬ－ＲＰＣは、できるだけ簡単になるように設計され、一方、複雑なデータ構造の伝送、処理及び返送を可能にする。

【０１３２】動的コンフィギュレーション機構を実現する実施例において、ユーザは、クライアント装置からサーバへ連絡し、ローカル・サーバ内のローカル・モジュールは、今のロケーションのクライアント・モジュールからのユーザにサービスを与えることが許されるかどうかを判定するため検査される。許されない場合、ローカル・サーバは、今のロケーションのクライアント・モジュールからのユーザを次にサポートするためにローカル・サーバを再構成すべきか、又は、更新すべきかを決定するため中央サーバと通信する。ローカル・モジュールが再構成された場合、ユーザ及びクライアント装置は認証され、ユーザのアクセス特権はアクセス可能な状態にされ、これにより、ユーザは、認証されたクライアント装置から保護文書にアクセスすることが許可される。

【０１３３】上記の実施例に続いて、唯一の局在化されたアクセス制御マネージメントを行うように、サーバ・モジュールの局在化されたバージョンを保持するため、一つ以上のローカル・サーバを利用する。図６Ｂは、１台以上のローカル・サーバに組み込まれ、アクセス制御マネージメントを動的に構成する処理６２０のフローチャートである。処理６２０は、図６Ａのステップ６１０及び６１２で実行される。ステップ６１０において、ユーザは、認証されていることが判定される。次に、ステップ６２２で、サーバは、ユーザが保護文書にアクセスすることが許可されているロケーションの数、又は、コンピュータの台数を判定する必要がある。動作中に、ユーザのアクセス特権が検査される．典型的に、ユーザのアクセス特権は、場所（例えば、許可されたロケーショ

ン、地理学的なロケーション、又は、ローカル・エリア・ネットワーク）、及び／又は、ユーザが利用可能なローカル・コンピュータ（例えば、許可されたコンピュータ）を識別する情報を含む。ある種のケースでは、ユーザは、幾つかの地理学的ロケーションにある数ヶ所のオフィスの間を頻繁に移動するので、ユーザは、それらの地理学的ロケーション／コンピュータの何れからでも保護文書にアクセスすることができる特権が与えられる。

【０１３４】ステップ６２４において、受け取られた要求元のユーザの現在ロケーションが、アクセス特権で許可されたロケーションであるかどうかを判定するため検査される。現在ロケーションが許可されたロケーションの中にない場合、処理６２０はステップ６２６へ進み、ユーザに通知を送信するか、又は、単に要求を拒絶する。現在ロケーションが許可されたロケーションの中に含まれる場合、処理６２０はステップ６２８へ進み、現時に局在化されたアクセス制御マネージメントを行うローカル・マネージャは、ユーザがそのローカル・マネージャによる局在化されたアクセス制御マネージメントの下にあるかどうかを判定するため検査される（例えば、図５Ａのローカル・サーバ・マネージャ５１４で）。ユーザがローカル・モジュールによる局在化されたアクセス制御マネージメントで制御されている場合、処理は、図６Ａのステップ６１２へ進む。ユーザがローカル・モジュールによる局在化されたアクセス制御マネージメントで制御されていない場合、サーバは、ステップ６３０で、局在化されたアクセス制御マネージメントを前にユーザへ提供していたローカル・モジュールはどれであるかを判定する必要がある。情報が種々のローカル・サーバのローカル・モジュールから収集された後、ローカル・モジュールの再構成がステップ６３２で行われる。本質的に、ユーザ支援は、図６Ｃに記載されているように、一方のローカル・モジュールから除去され、別のローカル・モジュールに追加される。

【０１３５】ステップ６３４において、新たに構成されたローカル・モジュールは、夫々、対応したローカル・サーバにアップロードされる。その結果として、ユーザは、新しいロケーションから保護文書にアクセスできるようになり、システムは、常に、一箇所のロケーション／コンピュータからのアクセスしか許可されないことが保証される。

【０１３６】ローカル・モジュールを動的に再構成する機構の特徴の一つは、図５Ａの中央サーバ５００による中央アクセス制御マネージメントの信頼性、確実性、及び、拡張性である。企業が多数のロケーションに多数の従業員を有する場合、ローカル・サーバは、性能を妥協することなく、ニーズを受け入れるために追加され得る。実際には、ユーザは、中央サーバとローカル・サーバとの間の夫々のコネクションが利用できない場合に、所定の期間中に殆ど影響されることがない。

【０１３７】図６Ｃは、一実施例に従ってローカル／モジュールを再構成する処理６４０のフローチャートである。処理６４０は、例えば、図６Ｂのステップ６３２で実行される処理である。ステップ６４２において、第１のロケーションで前にユーザを支援した第１のローカル・モジュールが識別される。ステップ６４４において、第１のローカル・モジュールは、第１のロケーションでのユーザに対するサポートを原則として除去するように構成される。次に、新しく構成された第１のローカル・モジュールが、ステップ６４６において、有効にされる対応したローカル・サーバへアップロードされ、その結果、ユーザはローカル・サーバでサポートされなくなる。ステップ６４８において、第２のロケーション（すなわち、ユーザの現在の居所）でユーザを支援するための第２のローカル・モジュールが識別される。ステップ６５０において、第２のローカル・モジュールは、本質的に、第２のロケーションでユーザにサポートを加えるため再構成される。新たに構成された第２のローカル・モジュールは、ステップ６５２で、有効になるべき対応したローカル・サーバへアップロードされ、ユーザはそのローカル・サーバでサポートされる。

【０１３８】保護文書へのユーザのアクセスの構成は、プロビジョニング処理と呼ばれることがある。上述の動的プロビジョニングは、中央サーバでの集中アクセス制御マネージメントを失うことなく、幾つかのロケーションに従業員を有する大企業によって要求される必要なセキュリティ手段を提供するものであると考えられる。更に、中央サーバを支援するため多数のローカル・サーバを使用することによって、信頼性、確実性、及び、拡張性を高めることが可能である。

【０１３９】図７Ａを参照するに、クライアント装置７００の機能ブロック図が示されている。クライアント装置７００は、主として、保護文書へアクセスするユーザが使用するコンピュータ装置である。クライアント装置７００は、例えば、デスクトップ型コンピュータ、携帯型装置、又は、ラップトップ型コンピュータでもよい。一実施例によれば、クライアント装置７００は、プロセッサ７０１と、クライアント・モジュール７０２と、メモリ空間７０３と、ネットワーク・インタフェース７０５と、ローカル記憶装置７０７と、を有する。クライアント・モジュール７０２は、メモリ空間７０３に置かれ、プロセッサ７０１によって実行されるときに、本発明において熟考された特徴、効果及び利点を実現する。ネットワーク・インタフェース７０５を介して、クライアント装置７００は、データネットワーク経由で、サーバのような他のコンピュータと通信する能力を備えている。クライアント装置７００から、ユーザは、リポジトリ（記憶装置）７０６に収容された保護文書にアクセスできる。リポジトリ７０６は、クライアント装置７００、別のネットワーク接続装置、或いは、その他の記憶

手段に設けられる。クライアント・モジュール７０２は、本発明の一実施例の実行可能バージョンである。一実施例によれば、クライアント・モジュール７０２は、アクセス報告モジュール７０４と、ユーザ照合用モジュール７１０と、鍵マネージャ７０８と、文書保護用モジュール７１１と、オフラインアクセスモジュール７１４と、を含む多数のサブモジュールを有する。

【０１４０】アクセス報告モジュール７０４について

このモジュールは、アクセス行動を記録するように構成されたソフトウェア・エージェントであり、認証されたユーザに関連付けられる。このモジュールは、中央サーバのアクセス報告モジュールへ報告するので、アクセスされた保護文書、アクセスしたユーザ、アクセスが行われた時間に関する記録が設定される。特に、アクセス報告モジュール７０５は、クライアント装置がネットワーク接続されていないときに、ユーザのアクセス行動を捕捉するため作動される。アクセス行動は、後で、サーバ内の対応する部分と同期させられ、オフラインアクセスのためのアクセス制御マネージメントが容易に行えるようになる。

【０１４１】鍵マネージャ７０８について

鍵マネージャ７０８の一つの目的は、保護文書が突然に停止するアプリケーションによってアクセスされているときに、保護文書が使用可能状態に保たれることを保証することである。一実施例によれば、暗号ヘッダが復号化された後、ファイル鍵がコピーされ、ファイル鍵のコピーは、鍵マネージャ７０８に保存（キャッシュ）される。ファイル鍵は、次に、暗号文書を復号化するため使用される。クリア文書がアプリケーションから利用できるようになる。アプリケーションが電源異常又は他のアプリケーション若しくはＯＳからの妨害によって停止した場合、ヘッダ内のファイル鍵が壊れる可能性がある。ファイル鍵のコピーが利用できない場合、暗号文書がファイル鍵無しでは復号化されないので、保護文書は使用できなくなる。この場合、鍵マネージャに保存されていた予備鍵が、損傷した鍵を置換し、暗号文書を復号化するため使用される。ユーザがファイルをもう一度保存した後、ファイル鍵はヘッダに戻される。鍵マネージャ７０８の別の目的は、認証されたユーザのユーザ鍵をキャッシュする（隠す）ことである。

【０１４２】ユーザ照合モジュール７１０について

このモジュールは、保護文書にアクセスしているユーザが認証されたかどうかを判定する役割を担い、認証されていない場合、ローカル・サーバ若しくは中央サーバによる認証のための要求を発動する。すなわち、ユーザ照合モジュール７１０は、保護文書へのアクセスを求めるユーザに許可を与える前に、常に調べられる。一実施例によれば、認証されたユーザのユーザ鍵は、ユーザがサーバを介してユーザ照合用モジュールによって認証された後、鍵マネージャ７０８に保存（キャッシュ）される。保護文書がアクセスされたとき、ユーザ鍵は、保護文書のヘッダ内の暗号セキュリティ情報を復号化するため、鍵マネージャ７０８から取り出されるべきである。

【０１４３】文書保護用モジュール７１１について

上述の如く、ＤＳＭ７１１は、ファイル鍵／ユーザ鍵を生成し、文書／ヘッダを暗号化／復号化するため使用される暗号器７１２を具備する。更に、他の保護用手段をＤＳＭ７１１に組み込んでもよい。他の保護用手段には、例えば、保護文書のコンテンツを非保護文書へコピーすることを防止するフィルタ、保護文書／オリジナルのソースから別の文書若しくは受け取り側ソースへのリンクが含まれる。

【０１４４】オフラインアクセス・マネージャ７１４について

このモジュールは、ネットワーク接続されたクライアント装置がネットワークから外れたとき、すなわち、ローカル・サーバ又は中央サーバが利用できないときに有効になる。例えば、ユーザが出張中であるとき、ラップトップ型コンピュータ内のある種の保護文書にアクセスする必要がある。ライブのコンサルテーションを利用できない場合、オフラインアクセス・マネージャ７１４が作動され、許可されたユーザは、依然として保護文書へアクセス可能であるが、時間が制限され、かつ、おそらく、特権が制限されていることを保証する。

【０１４５】図７Ａのクライアント・モジュール７０２は、本発明の一実施例による例示的なサブモジュールを列挙したものであり、本発明を実施するためには、必ずしもサーバ・モジュール７０２内の全てのモジュールを組み込まなくてもよいことに注意する必要がある。ここでの記述から当業者には明らかであるように、サブモジュールの多様な組み合わせは、本発明において熟考されたある種の機能、利益及び効果を達成するであろう。

【０１４６】クライアント・モジュール７０２の動作の多数の局面については既に説明した通りである。クライアント・モジュール７０２は、ユーザが、サーバ（すなわち、中央サーバ若しくはローカル・サーバ）に対して離れた場所にある保護文書に関する作業ができるようにするため、オフラインアクセス機能を提供する。サーバ（中央サーバ若しくはローカル・サーバのいずれか一方）に対する依存性は、最小限に抑えられるので、機能が移動ユーザにも均等に適用される。図７Ｂを参照するに、本発明の一実施例によるオフラインアクセス提供処理７２０のフローチャートが示されている。

【０１４７】ユーザがある期間だけコンピュータの環境から離れることを決め、かつ、自分が携帯するつもりのクライアント装置（例えば、ラップトップ型コンピュータ）のある種の保護文書にアクセスする必要がある場合、ユーザは、ネットワークからクライアント装置を切り離す前にサーバから事前認証を受ける。ステップ７２２において、サーバ（例えば、中央サーバ又はローカル

・サーバ）からオフラインアクセス要求の承認を求めるため、事前認証要求がクライアント装置で行われる。厳密な実施態様に応じて、サーバから受け取られた事前要求に対する応答は、サーバがオフラインアクセス要求について処理を進めるためユーザからの更なる情報を要求するダイアログ・ボックスである。

【０１４８】ステップ７２４において、ユーザは、必要な情報を、特定の時間区間、ユーザの識別情報を含むオフラインアクセス要求に入力する。おそらく、オフラインアクセス要求は、オフラインでアクセスされる保護文書、又は、保護文書が収容される保護ディレクトリ／フォルダの名前を含む。一般的に、特定の時間が手入力され、或いは、選択されるが、ユーザの識別情報は自動的に入力される。なぜならば、ユーザは典型的に事前に認証され、クライアント装置はユーザの識別情報を得ているからである。オフラインアクセス要求は、次に、サーバへ転送され、サーバでは、オフラインアクセス要求が処理される。ユーザは、このようなオフラインアクセス特権を受けることが許可されている場合を想定する。

【０１４９】動作中に、オフラインアクセス機能を許可するために多数の方法が考えられる。一例の方法は、時間制限の厳しいアクセス修正を望ましい保護文書に収容することである。例えば、ユーザは、新たに生成された短期ユーザ鍵のペアを許可することにより事前認証され、或いは、ユーザの鍵を解読できないフォーマットでクライアント装置へアップロードすることによって事前認証される（保護文書だけにアクセスする場合には秘密鍵だけが必要であり、新たに作成された文書を保護するためには両方の鍵が必要である。）。換言すると、ユーザのアクセス特権、又は、選択された保護文書内のアクセス規則は、要求された期間に亘って更新される。従って、実現形態に応じて、修正されたアクセス規則、修正されたアクセス特権、又は、時間制限の厳しいユーザ鍵が、ステップ７２６において、サーバ７２６から受け取られる。

【０１５０】ステップ７２８において、元のアクセス規則、又は、ユーザの元のアクセス特権、又は、元のユーザ鍵が修正、更新、或いは、一時的に上書きされる。修正されたアクセス規則が受け取られたとき、保護文書はアクセス規則に補正を取り込むため処理され、その結果として、ユーザは、後で、オフラインのときであっても、この保護文書にアクセスすることができる。修正されたアクセス特権が受け取られたとき、ユーザの元のアクセス特権は、受け取られた修正を用いて一時的に改訂されるので、ユーザは、保護文書にオフラインでアクセスすることが可能になる。時間制限の厳しいユーザ鍵が受け取られたとき、ユーザの元の鍵は保留され（例えば、解読できないフォーマットに変換され、容易には使用できなくなる。）、新たに受け取られた鍵がオフラインアクセス期間だけ有効にされる。図７Ｃには、アクセス規則の補正がユーザＡ、Ｂ、Ｃ及びＤによってアクセス可能な保護文書に入れられ、ユーザＡがオフラインアクセスを要求し、その要求に対してオフラインアクセスが許可され、ユーザＢ、Ｃ及びＤは、その保護文書にオフラインでアクセスし得ない状況が示されている。

【０１５１】セキュリティ上の理由から、補正は、典型的に、ユーザが戻ったか戻っていないかとは無関係に、特定のオフライン時間の終了によって期限が切れる。この特徴は、クライアント装置（例えば、ラップトップ型コンピュータ）がユーザから離れているか、又は、許可されていない人によって所持されているような状況において重要だえる。なぜならば、クライアント装置内の保護文書は、たとえ、ユーザの資格情報（ユーザ名／パスワード）が盗まれているとしても、失効したユーザ鍵を用いてアクセスできなくなっているからである。したがって、ステップ７３０において、処理７２０は、オフライン時間が終了したかどうかを検査し続ける。オフライン時間が終了していない場合、ユーザは、依然として、保護文書にオフラインでアクセスすることが可能である。オフライン時間の満了が検出されたとき、処理７２０はステップ７３４へ進み、元のアクセス規則は復元され、保護文書はオフラインでアクセスできなくなる。

【０１５２】同様に、ユーザの修正されたアクセス特権は、オフライン時間の終了が検出されたときに失効するように設定され、処理７２０はステップ７３４へ進み、ユーザの元のアクセス特権が復元されるので、保護文書はオフラインでアクセスできなくなる。一実施例によれば、修正されたアクセス特権は、元のアクセス特権によって上書きされる。

【０１５３】ユーザが自分の旅行を短縮した状況を考慮するため、処理７２０は、保護文書に対する元の設定値、又は、ユーザのアクセス特権の復元を開始するように構成してもよい。ステップ７３２において、クライアント装置は、アクセス制御サーバへのコネクションが確立され、それにより、オフラインアクセスはそれ以上必要ではなくなった場合を考える。処理７２０は、ステップ７３４へ進み、保護文書に対する元の設定値、ユーザのアクセス特権、又は、ユーザ鍵の復元が行われる。その結果として、保護文書は、クライアント装置からオフラインではアクセスできなくなる。

【０１５４】何れのケースでも、好ましくは、オフラインアクセス期間中のユーザによるアクセス行動を記録するため、クライアント・モジュール７０２のアクセス報告モジュール７０４が呼び出される。次に、ユーザがサーバへ接続したとき、保護文書のアクセス行動はサーバへ報告され、オフライン期間中にアクセスされた保護文書のアクセス制御マネージメント又は同期が容易に実現される。

【０１５５】本発明には、多数の機能、利益及び効果がある。機能、利益及び効果のうちの一つは、本発明にお

いて熟考された保護用機構が、保護されたデジタル資産のアクセス規則を利用することによって、常に、選択されたデジタル資産を保護状態に保つことである。このようにして、認証された装置と許可されたユーザだけが保護デジタル資産にアクセス可能である。他の機能、利益及び効果は、詳細な説明を参照することによって当業者に明らかである。

【０１５６】本発明は、方法、システム、コンピュータ読み取り可能な媒体、プログラム、コンピュータ製品、及び、望ましい態様を実施するその他の形態として実現することが可能である。当業者に明らかであるように、以上の説明は、記載された様々な組み合わせ、実施例、若しくは、設定状況に関して、他の多種多様な設定状況に同じように適用され、或いは、使用される。

【０１５７】上述の処理、シーケンス又はステップ、及び、機能は、相互に関連し、各々は個別に新規性を備えていると考えられる。開示された処理、シーケンス又はステップ、及び、機能は、単独で実行することが可能であり、或いは、新規性があり自明ではないシステム若しくはシステムの一部を与えるために組み合わせて実行することが可能である。処理、シーケンス又はステップ、及び、機能を組み合わせることにより、たとえ、最広義の組み合わせであっても、すなわち、処理、シーケンス又はステップ、及び、機能の各々が実施のために縮小された特定の態様に満たない場合であっても、同等に独立した新規性のある組み合わせが同時に得られることに注意する必要がある。

【０１５８】上記実施例の説明は、本発明の種々の局面／実施例の例示に過ぎない。本発明に関する様々の変更は、特許請求の範囲に記載された発明の真の精神及び範囲を逸脱することなく、当業者によってなされるであろう。したがって、本発明の範囲は、上記の実施例の説明ではなく、特許請求の範囲に記載された事項によって定められる。

【図面の簡単な説明】

【図１Ａ】本発明の好ましい一実施例による基本システムの構成図である。

【図１Ｂ】中央サーバ及びローカル・サーバが利用されたシステムの構成図である。

【図１Ｃ】ローカル・サーバの利用されない小グループのユーザに適したシステムの構成図である。

【図１Ｄ】本発明が導入され実行されるコンピュータ装置（例えば、クライアント装置、中央サーバ及びローカル・サーバ）の内部構成ブロック図である。

【図２Ａ】作成文書の保護処理の説明図である。

【図２Ｂ】ヘッダ及び暗号データ部を含む保護文書の構造の一例の説明図である。

【図２Ｃ．１】ヘッダ及び暗号部に多数のユーザ情報を収容する保護文書の構造の別の例の説明図である。

【図２Ｃ．２】ヘッダ及び暗号部にセキュリティブロックを収容する保護文書の構造の更に別の例の説明図である。

【図２Ｃ．３】図２Ｃ．２に示された保護文書の構造に対応したマークアップ言語によるヘッダの例の説明図である。

【図２Ｄ】ユーザがアクセス規則を設定若しくは作成するため使用されるグラフィカル・ユーザ・インタフェース（ＧＵＩ）の一例の説明図である。

【図２Ｅ】クリアフォルダ及び保護（使用中）フォルダを含むディレクトリ構造の説明図であり、クリアフォルダは一般的にシステムファイル又は保護が予定されていないファイルを記憶するためのフォルダであり、保護フォルダは保護形式のデータファイル及び文書のためのフォルダである。

【図３】オペレーティングシステム（例えば、WINDOWS（登録商標） 2000）と相互作用し内部で動作する文書保護用モジュールが保護された文書をユーザに気付かれないようにする方法の一実施例の説明図である。

【図４Ａ】本発明の一実施例により作成中文書を保護する処理のフローチャートである。

【図４Ｂ】文書保護処理を容易に実現するため図４Ａの処理に組み込まれ、アクセス規則を取得する処理の一例のフローチャートである。

【図４Ｃ】一実施例により保護文書にアクセスする処理のフローチャートである。

【図５Ａ】サーバ・モジュールがメモリ空間に存在し、１個以上のプロセッサによって実行可能にされている（アクセス制御）サーバ装置の機能ブロック図である。

【図５Ｂ．１】ユーザに対するアクセス特権の一例の説明図である。

【図５Ｂ．２】本発明の一実施例によるユーザ鍵マネージャの内容の説明図である。

【図５Ｂ．３】ユーザ鍵更新処理のフローチャートである。

【図５Ｂ．４】一実施例による保護文書アクセスのサーバ支援処理のフローチャートである。

【図５Ｂ．５】一実施例による文書保護のサーバ支援処理のフローチャートである。

【図５Ｃ】図５Ａに示されたサーバと多数の点で類似しているローカル・サーバ装置の機能ブロック図である。

【図５Ｄ】中央サーバによって管理された種々のアクセス特権が与えられた全ユーザの表の説明図である。

【図５Ｅ】ユーザは対応したローカル・サーバに問い合わせるだけでよく、他のローカル・サーバが如何なる理由で停止していても、或いは、中央サーバから切り離されていても影響されないように、ローカル・サーバによってアクセスされるそれぞれの表の説明図である。

【図５Ｆ】Johnが３箇所のどこからでもアクセスできるように３個の同一のキャッシュモジュールを設けるのではなく、Johnが同時に３箇所のロケーションのうちの１

箇所からだけアクセスできるように１個のキャッシュモジュールだけが構成されている、各ユーザに関するアクセス可能性の説明図である。

【図５Ｇ】他の場所から移動してきたJohnのために機能することができる別のキャッシュモジュールにJohnを追加することによる動的キャッシュ用アクセス制御マネージメントの説明図である。

【図５Ｈ】動的キャッシュ用アクセス制御マネージメントの結果として変更されるユーザのアクセス可能性の説明図である。

【図５Ｉ】動的キャッシュ用アクセス制御マネージメントの結果として変更されるユーザのアクセス可能性の説明図である。

【図６Ａ】中央サーバ又はローカル・サーバに組み込まれるユーザ認証処理のフローチャートである。

【図６Ｂ】中央サーバと共に１台以上のローカル・サーバに組み込まれるアクセス制御マネージメント処理の動的構成のフローチャートである。

【図６Ｃ】図６Ｂに使用される一実施例によるローカルモジュール処理の再構成のフローチャートである。

【図７Ａ】本発明を実施するため使用されるクライアント装置の機能ブロック図である。

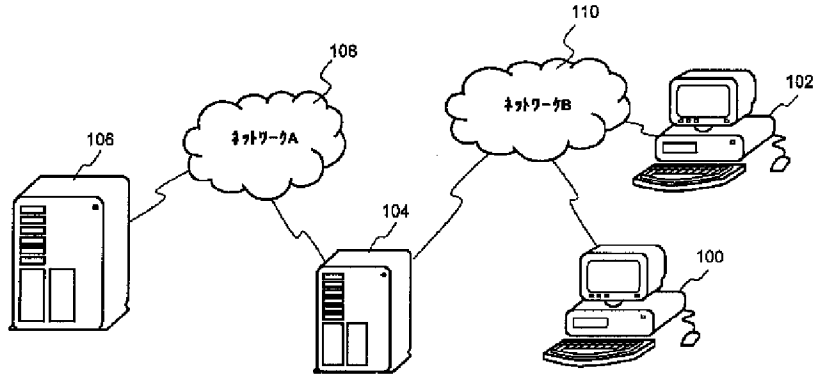
【図７Ｂ】本発明の一実施例によるオフラインアクセス処理のフローチャートである。

【図７Ｃ】ユーザＡ、Ｂ、Ｃ及びＤによってアクセス可能な保護文書に収容されたアクセス規則の修正の説明図であり、ユーザＡはオフラインアクセスを要求してその要求を許可され、ユーザＢ、Ｃ及びＤは保護文書にオフラインでアクセスできない。

【符号の説明】

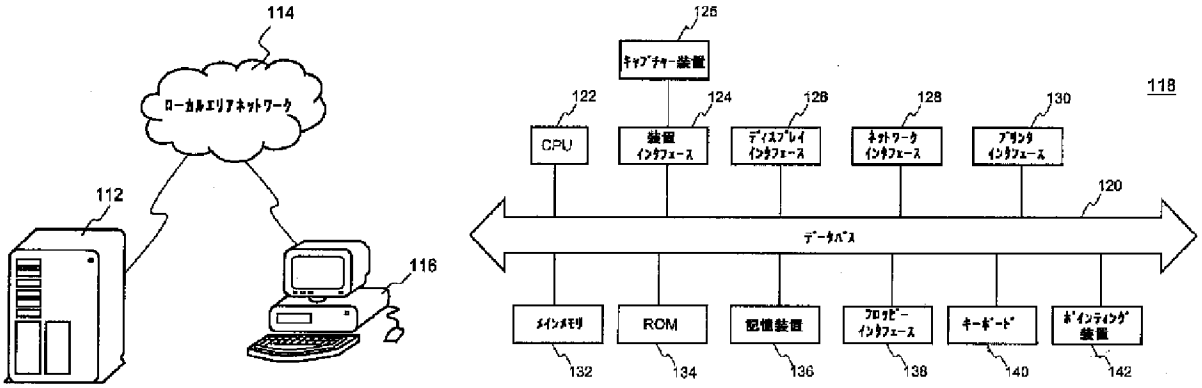
５０１　プロセッサ
５０２　サーバ・モジュール
５０３　メモリ
５０４　ネットワーク・インタフェース
５０５　ローカル記憶装置
５０６　管理インタフェース
５０７　データベース
５０８　アカウント・マネージャ
５１０　ユーザ鍵マネージャ
５１２　ユーザ・モニタ
５１６　パートナー・アクセス・マネージャ
５１８　アクセス報告
５２０　オプションモジュール
５１４　ローカル・サーバ・マネージャ

【図１Ａ】

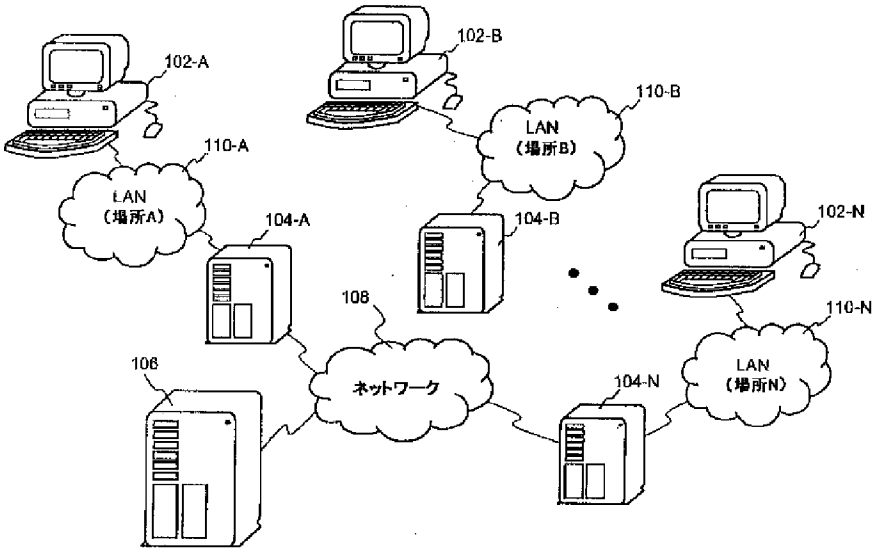


【図１Ｃ】

【図１Ｄ】

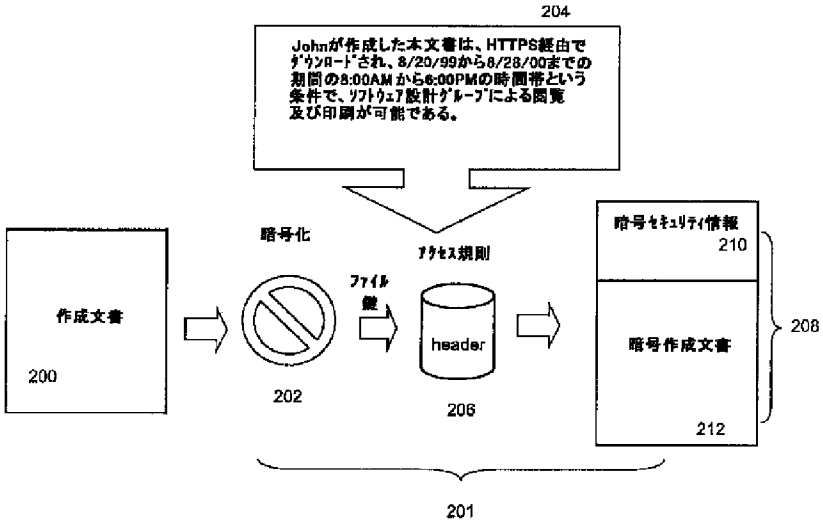


【図１Ｂ】

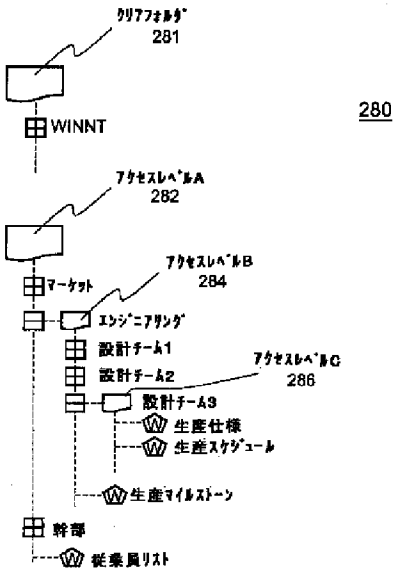


【図２Ａ】

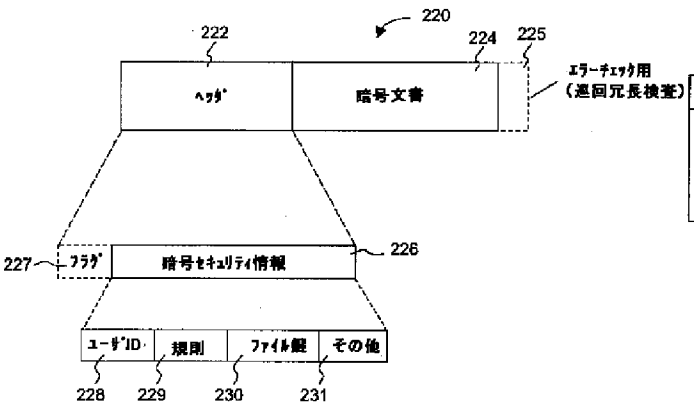
【図２Ｅ】



【図２Ｂ】

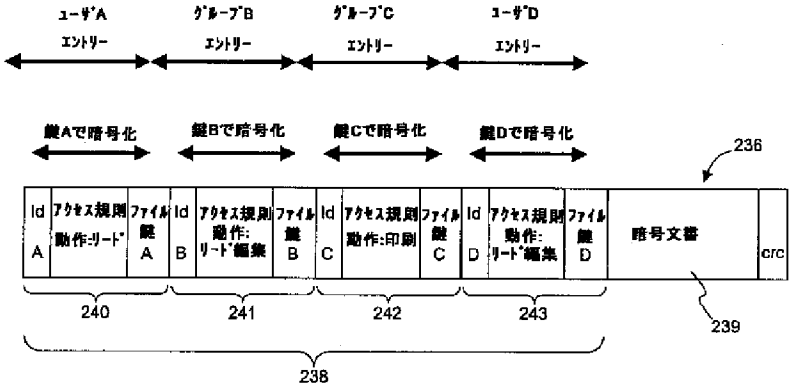


【図５Ｂ．２】

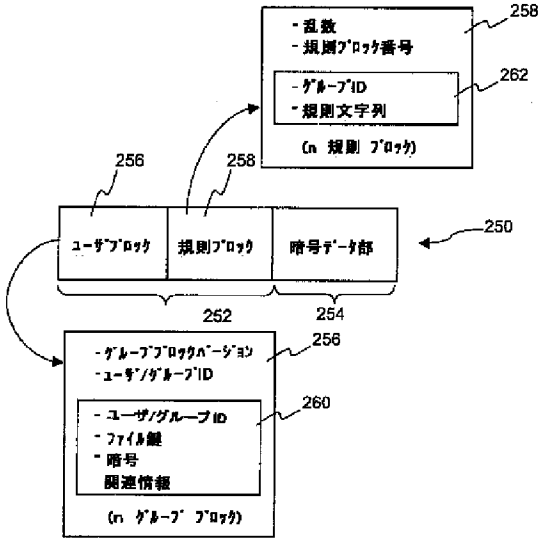


全ﾕｰｻﾞ鍵	鍵／鍵ﾍﾞｱ	ﾛｹｰｼｮﾝ	その他
John	111101101010101	128.1.100.64, ...	
Mike , Dell	101011000111111	64.100.1.128, ...	
金融ｸﾞﾙｰﾌﾟ	010101010111111	64.100.1.100, ...	
● ● ●			

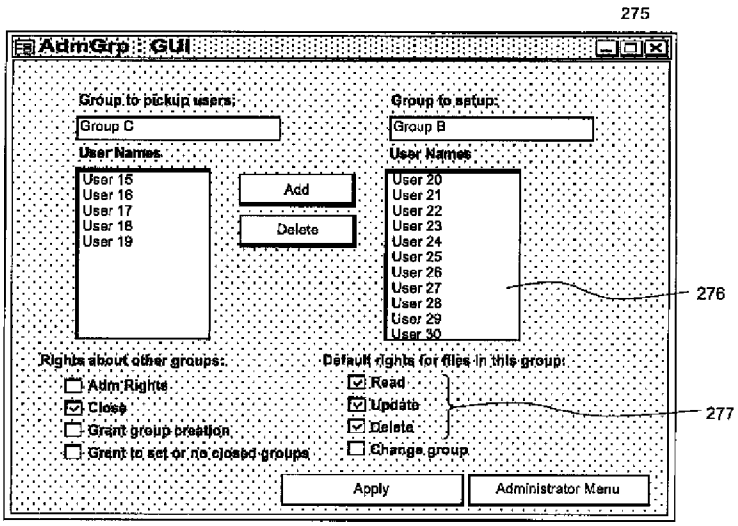
【図２Ｃ．１】



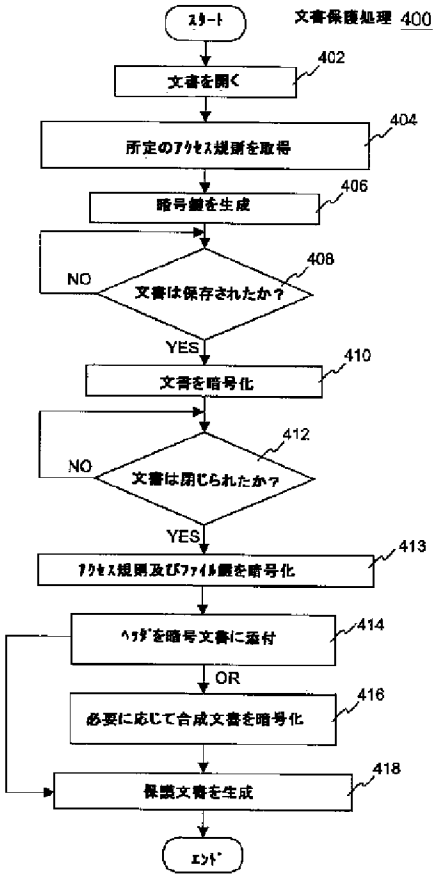
【図２Ｃ．２】



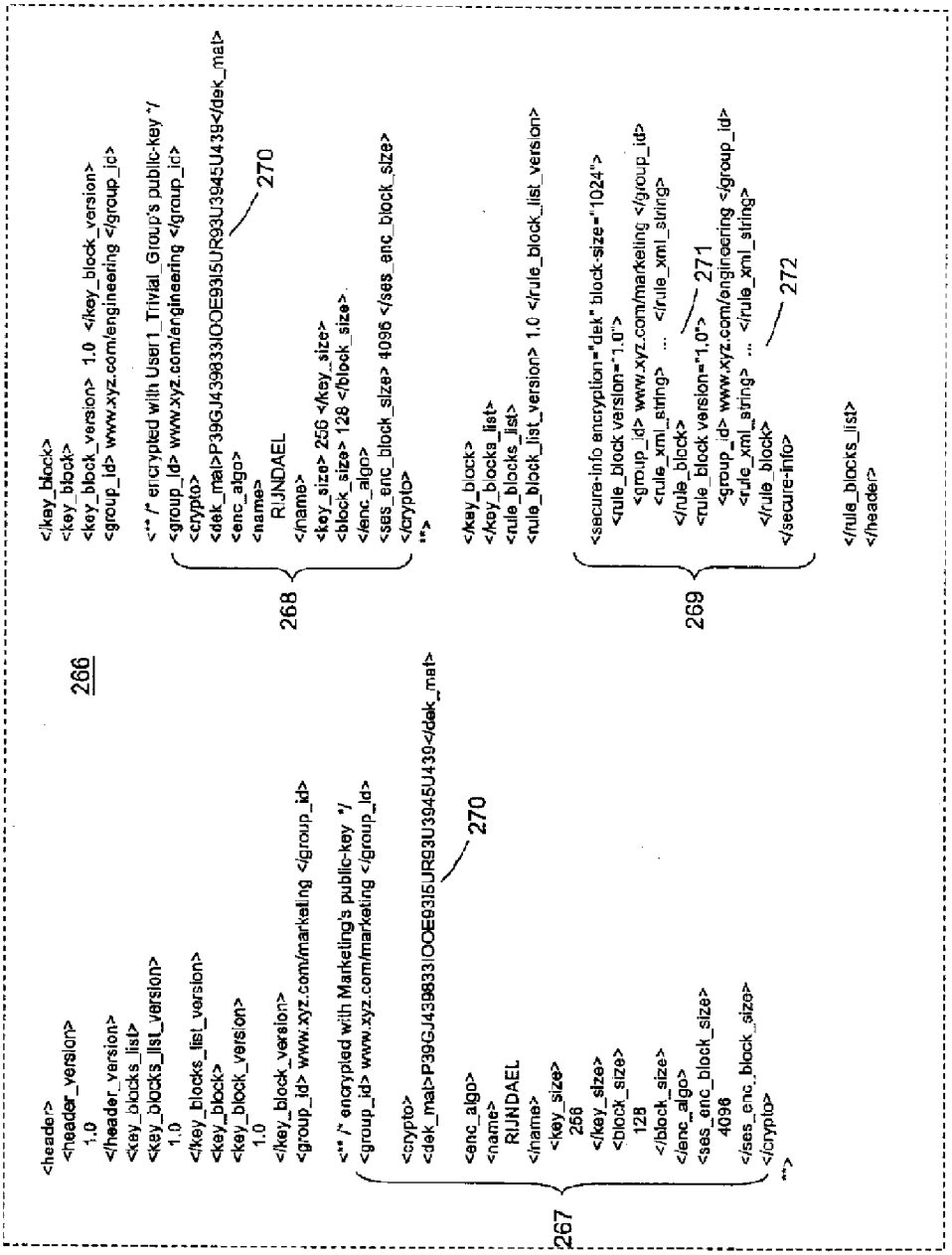
【図２Ｄ】



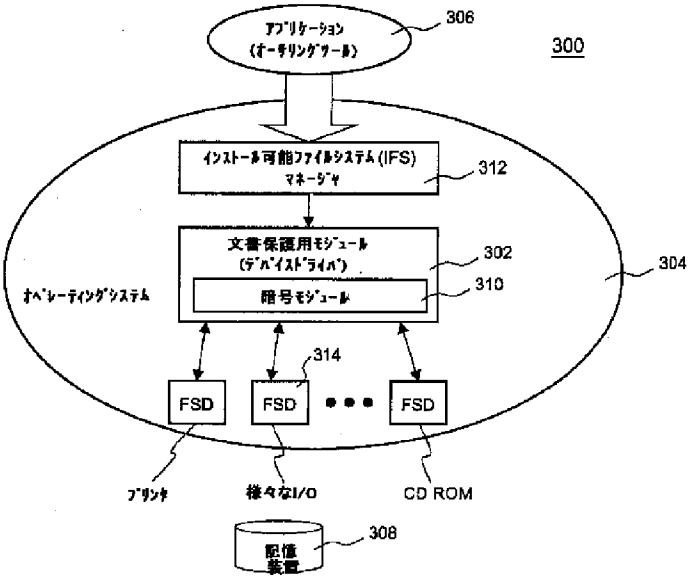
【図４Ａ】



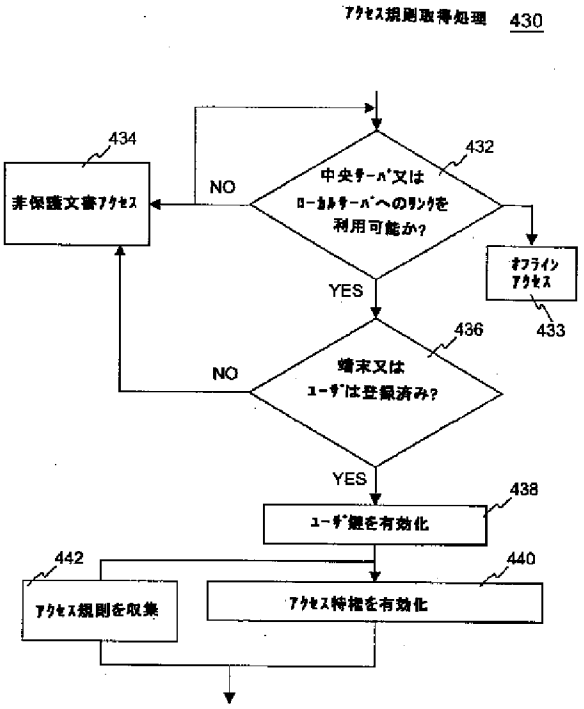
【図２Ｃ．３】


<header>
<header_version>
1.0
</header_version>
<key_blocks_list>
<key_blocks_list_version>
1.0
</key_blocks_list_version>
<key_block>
<key_block_version>
1.0
</key_block_version>
<group_id> www.xyz.com/marketing </group_id>
<!* /* encrypted with Marketing's public-key */
<group_id> www.xyz.com/marketing </group_id>
<crypto>
<dek_mat>P39GJ439833IOOE93I5UR93U3945U439</dek_mat>
270
<enc_algo>
<name>
RIJNDAEL
</name>
<key_size>
256
</key_size>
<block_size>
128
</block_size>
<enc_algo>
<ses_enc_block_size>
4096
</ses_enc_block_size>
</crypto>
*>
267
266
</key_block>
<key_block>
<key_block_version> 1.0 </key_block_version>
<group_id> www.xyz.com/engineering </group_id>
<!* /* encrypted with User1_Trivial_Group's public-key */
<group_id> www.xyz.com/engineering </group_id>
<crypto>
<dek_mat>P39GJ439833IOOE93I5UR93U3945U439</dek_mat>
270
<enc_algo>
<name>
RIJNDAEL
</name>
<key_size> 256 </key_size>
<block_size> 128 </block_size>
</enc_algo>
<ses_enc_block_size> 4096 </ses_enc_block_size>
</crypto>
*>
268
</key_blocks>
</key_blocks_list>
<rule_blocks_list>
<rule_block_list_version> 1.0 </rule_block_list_version>
<secure-info encryption="dek" block-size="1024">
<rule_block version="1.0">
<group_id> www.xyz.com/marketing </group_id>
<rule_xml_string> ... </rule_xml_string>
</rule_block>
<rule_block version="1.0">
271
<group_id> www.xyz.com/engineering </group_id>
<rule_xml_string> ... </rule_xml_string>
</rule_block>
</secure-info>
272
269
</rule_blocks_list>
</header>

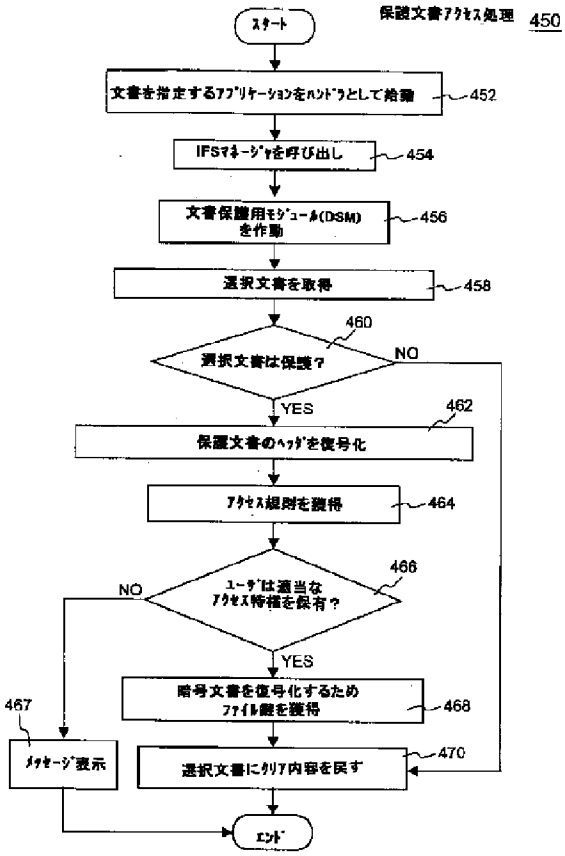
【図３】


アプリケーション
(オーサリングツール)
306
300
インストール可能ファイルシステム(IFS)
マネージャ
312
文書保護用モジュール
(デバイスドライバ)
302
暗号モジュール
310
304
オペレーティングシステム
314
FSD
FSD
FSD
プリンタ
様々なI/O
CD ROM
記憶装置
308

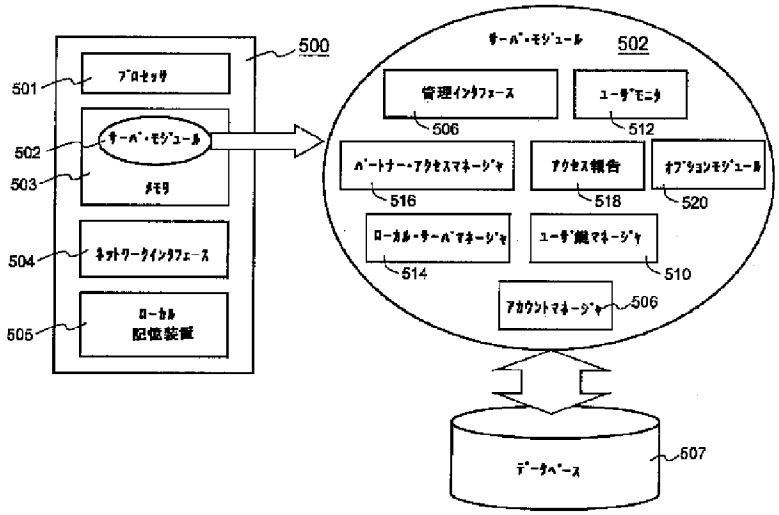
【図４Ｂ】


アクセス規則取得処理
430
434
非保護文書アクセス
NO
中央サーバ又は
ローカルサーバへのリンクを
利用可能か?
432
オフライン
アクセス
433
YES
436
端末又は
ユーザは登録済み?
NO
YES
438
ユーザ鍵を有効化
442
アクセス規則を収集
440
アクセス特権を有効化

【図４Ｃ】


スタート
保護文書アクセス処理
450
文書を指定するアプリケーションをハンドラとして始動
452
IFSマネージャを呼び出し
454
文書保護用モジュール(DSM)
を作動
456
選択文書を取得
458
460
選択文書は保護?
NO
YES
462
保護文書のヘッダを復号化
アクセス規則を獲得
464
466
ユーザは適当な
アクセス特権を保有?
NO
YES
暗号文書を復号化するため
ファイル鍵を獲得
468
467
メッセージ表示
選択文書にクリア内容を戻す
470
エンド

【図５Ａ】



【図５Ｂ．１】

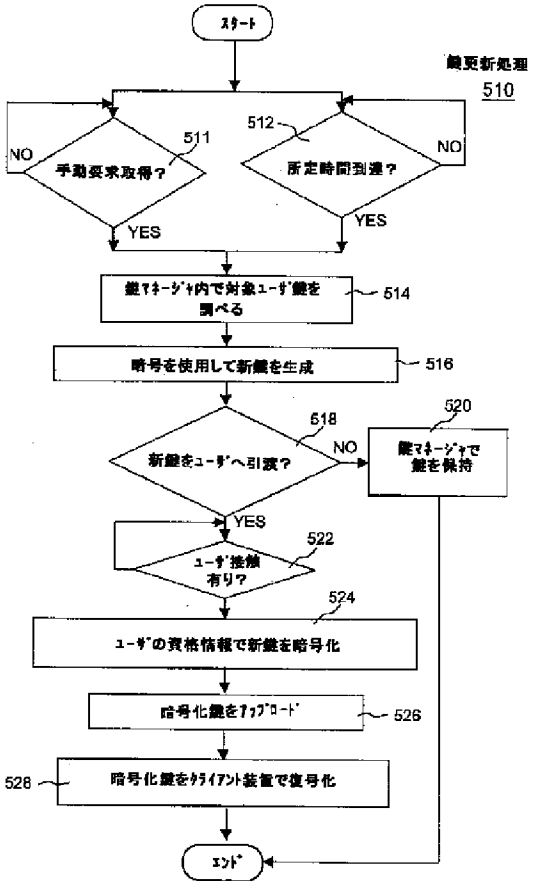
ユーザID	ユーザ	開く	編集	書込	印刷	コピー	ダウンロード	その他
01243	ユーザA	Y	Y	Y	Y	Y	Y	Y
17364	ユーザB	Y			Y			
18465	Gユーザ'C	Y	Y	Y			Y	
				• • •				

【図５Ｄ】

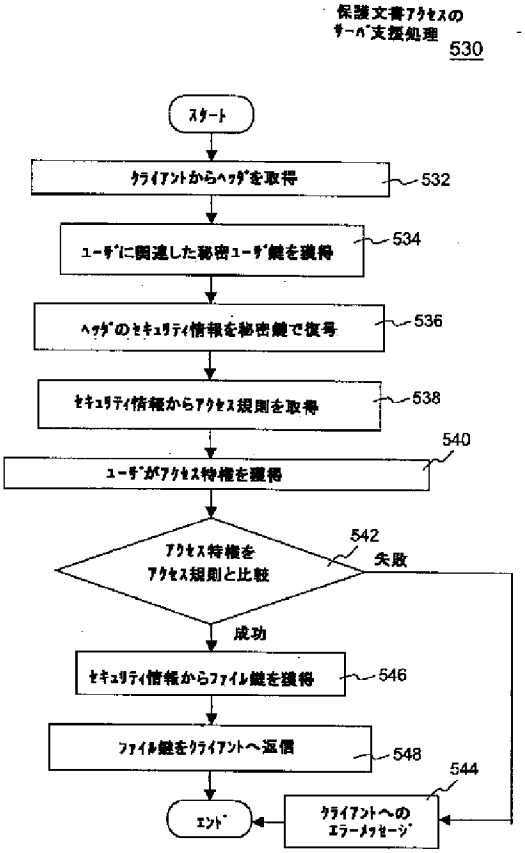
584

ユーザ	パスワード	アクセス特権	
John	*********	L=10, T=24, D=ALL, C=ALL	585
Dell	*********	L=1, T=8, D=M-F, C=A	586
Mike	*********	L=5, T=12, D=M-S, C=A & B	587
	• • •		

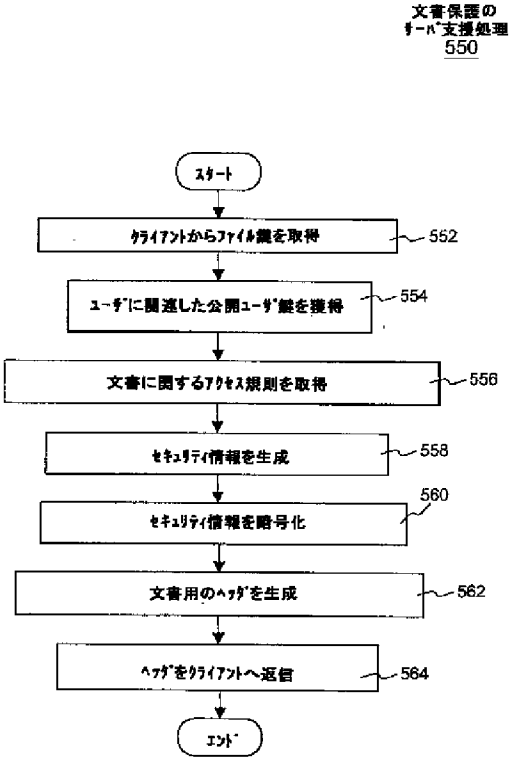
【図５Ｂ．３】



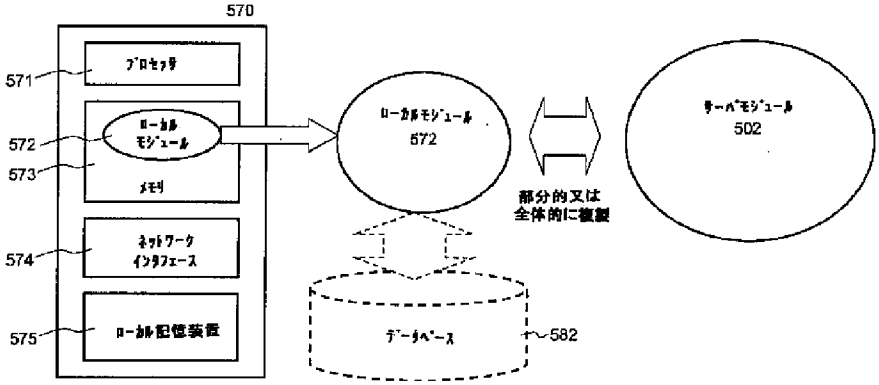
【図５Ｂ．４】



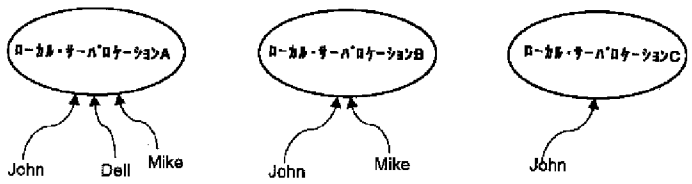
【図５Ｂ．５】



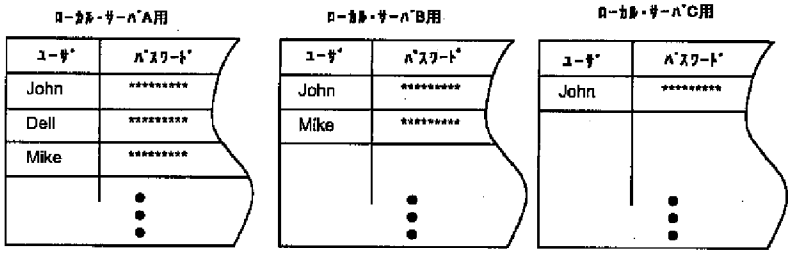
【図５Ｃ】



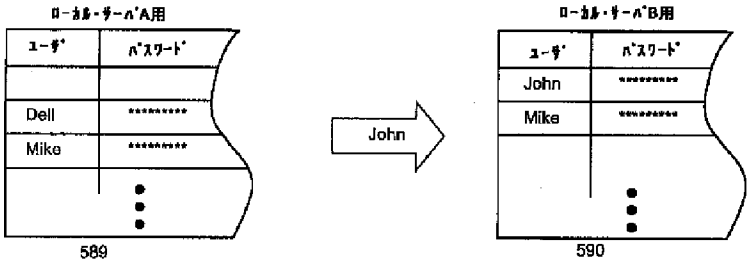
【図５Ｆ】



【図５Ｅ】

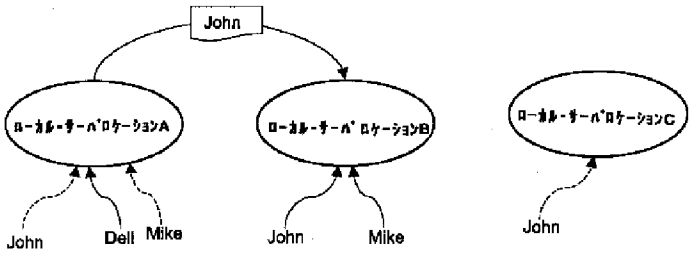


【図５Ｇ】

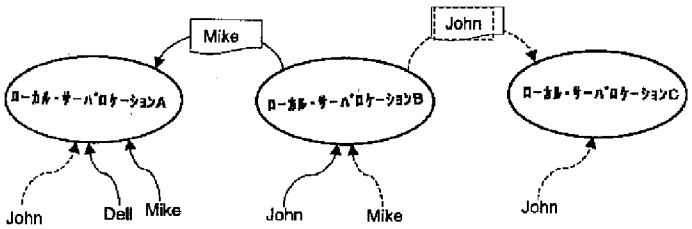


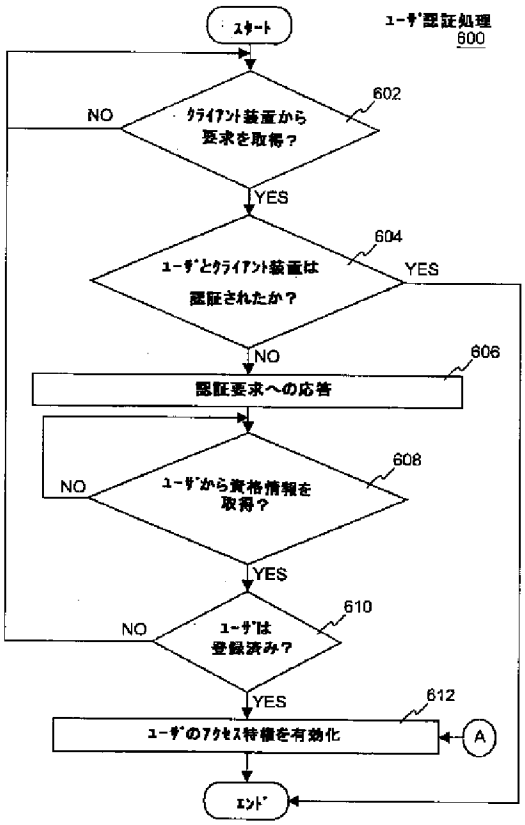
【図５Ｈ】

【図６Ａ】

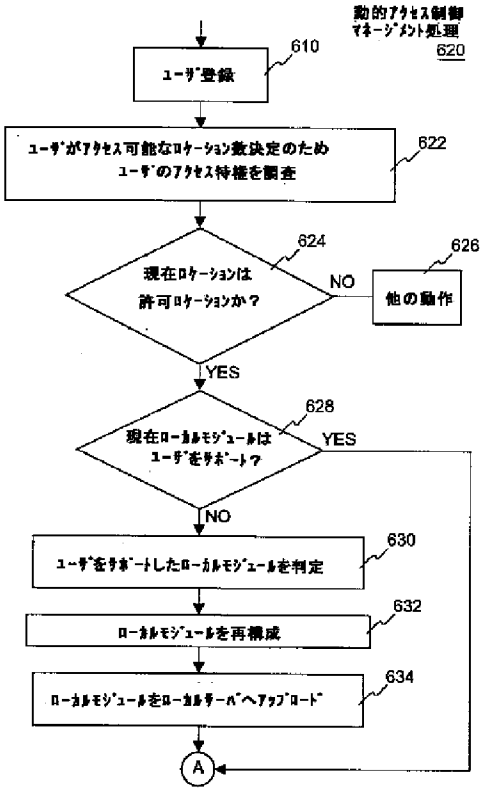


【図５Ｉ】

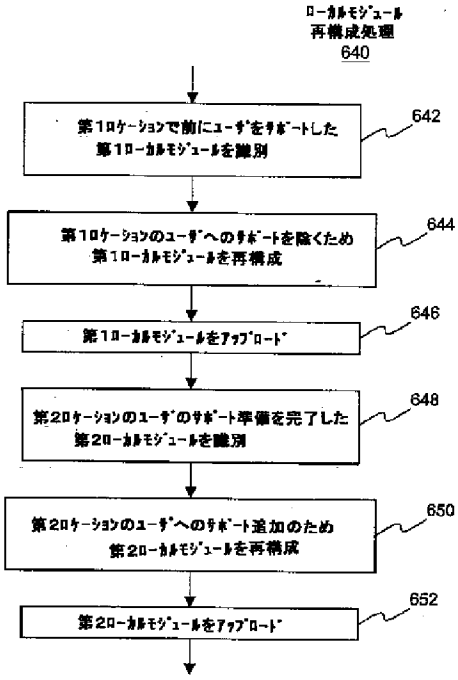




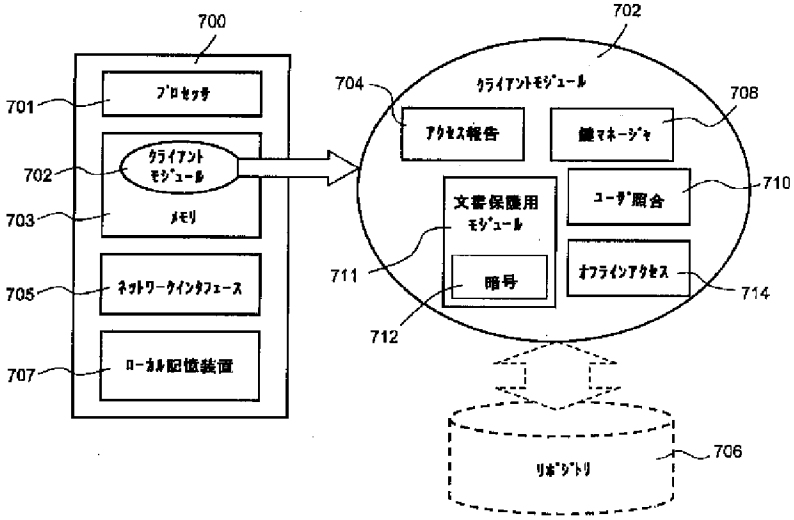
【図６Ｂ】


動的アクセス制御
マネージメント処理
620
610
ユーザ登録
622
ユーザがアクセス可能なロケーション数決定のため
ユーザのアクセス特徴を調査
624
現在ロケーションは
許可ロケーションか？
NO
626
他の動作
YES
628
現在ローカルモジュールは
ユーザをサポート？
YES
NO
630
ユーザをサポートしたローカルモジュールを判定
632
ローカルモジュールを再構成
634
ローカルモジュールをローカルサーバへアップロード
A

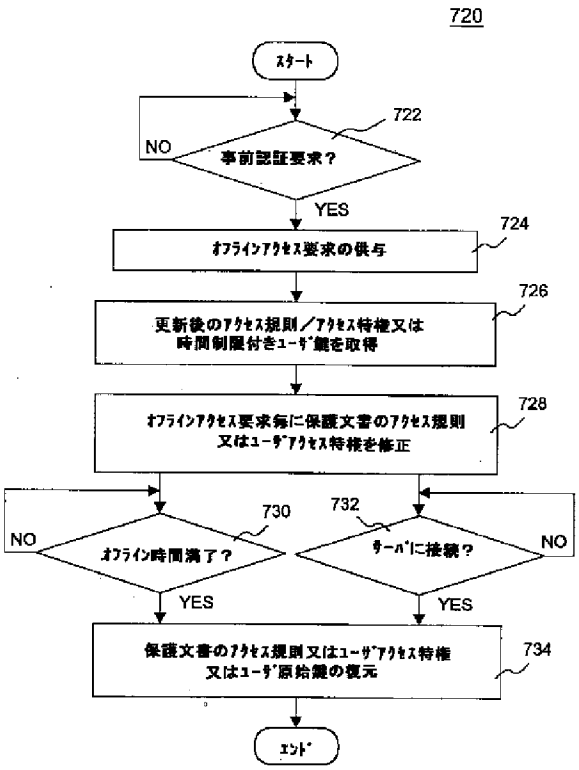
【図６Ｃ】


ローカルモジュール
再構成処理
640
642
第1ロケーションで前にユーザをサポートした
第1ローカルモジュールを識別
644
第1ロケーションのユーザへのサポートを除くため
第1ローカルモジュールを再構成
646
第1ローカルモジュールをアップロード
648
第2ロケーションのユーザのサポート準備を完了した
第2ローカルモジュールを識別
650
第2ロケーションのユーザへのサポート追加のため
第2ローカルモジュールを再構成
652
第2ローカルモジュールをアップロード

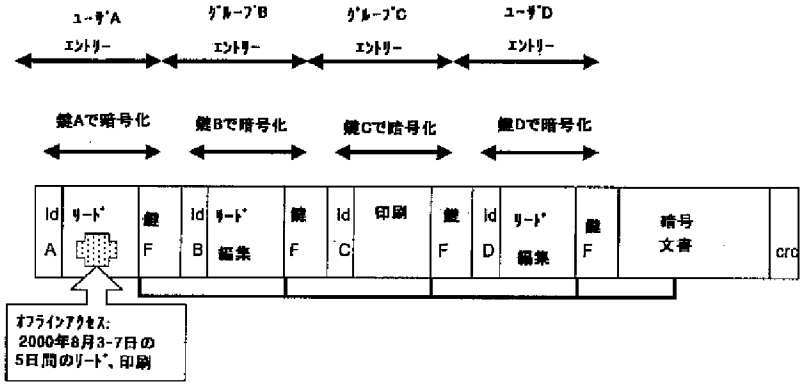
【図７Ａ】


700
701
プロセッサ
702
クライアント
モジュール
703
メモリ
705
ネットワークインタフェース
707
ローカル記憶装置
702
クライアントモジュール
704
アクセス報告
708
鍵マネージャ
文書保護用
モジュール
710
ユーザ照合
711
暗号
712
オフラインアクセス
714
706
リポジトリ

【図７Ｂ】



【図７Ｃ】



フロントページの続き

(51)Int.Cl.[7]	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ 9/08		Ｈ０４Ｌ 9/00	６０１Ａ	
9/32			６７３Ａ	

(72)発明者　アラン　ロスマン
アメリカ合衆国　カリフォルニア州　94301　パロ・アルト　カウパー・ストリート　1247
(72)発明者　パトリック　ジュイユ
アメリカ合衆国　カリフォルニア州　94306　パロ・アルト　トウル・ウェイ　696　アパートメント・39
(72)発明者　マイケル　ミチオ　オウイェ
アメリカ合衆国　カリフォルニア州　94022　ロス・アルトス　ウェスト・エディス・アヴェニュー　150　17号
(72)発明者　セルジュ　ユミシュ
フランス国　77220　トゥールナンーアンーブリ　ドメーヌ・ド・クールセル（番地なし）
(72)発明者　チャンーピン　リー
アメリカ合衆国　カリフォルニア州　94303　パロ・アルト　サン・アントニオ・ロード　765　アパートメント・65
(72)発明者　クリメンティー　ヴェインシュタイン
アメリカ合衆国　カリフォルニア州　95014　キュパーティーノ　ノース・フットヒル・ブールヴァード　10526　A号
(72)発明者　ハル　ヒルデブランド
アメリカ合衆国　カリフォルニア州　94038　モス・ビーチ　シエラ・ストリート　655
(72)発明者　デニス　ジャック　ポール　ガルシア
アメリカ合衆国　カリフォルニア州　94304　パロ・アルト　オーク・クリーク・ドライヴ　1736　アパートメント・204号
(72)発明者　センティルヴァサン　スプラマニアム
アメリカ合衆国　カリフォルニア州　94070　サン・カルロス　エルム・ストリート　520　アパートメント・26
(72)発明者　ウェイチン　ホアン
アメリカ合衆国　テキサス州　75022　フラワー・マウンド　アパラチアン・ウェイ　3705
(72)発明者　ニコラス　マイケル　ライアン
アメリカ合衆国　カリフォルニア州　99087　サニーヴェイル　ベルフェア・コート　795
Fターム(参考)　5B017 AA02 AA03 BA06 BB06 CA16
5B082 EA11
5B085 AE02 AE23 AE29 BG04 BG07
5J104 AA07 KA01 PA07